PerfectMail
Administrator's Guide

Version: 3.7.210
May 6, 2022

Contents

Contents

Contents

Contents

Contents

1 Copyright Notice

2 Welcome to PerfectMail™

Welcome to the *PerfectMail™ Anti-Spam Solution*. PerfectMail is an *Edge Transport Server* product that filters e-mail *before* it reaches your Mail Server. We provide a flexible solution that works with all SMTP based e-mail products; including Microsoft Exchange™, Lotus Domino™, Novell GroupWise™, Sendmail™, QMail™, etc. PerfectMail™ is a complete server product that can be installed on most modern hardware and virtualized environments.

Our focus is on *business e-mail*. Our mantra is: **No False Positives**!

2.1 Live Filtering

PerfectMail™ is a *live filtering solution*. E-mail is actively filtered, in real-time, during transmission. The e-mail transmission results in either an *accept* or *reject* status.

- *Accepted* e-mail is always delivered to the recipient... always!
- *Rejected* e-mail is always rejected during transmission.

Rejecting e-mail during transmission has some significant benefits for our customers. We accept or reject a message during the SMTP exchange between mail servers. This means we can leverage the existing e-mail infrastructure to *guarantee* the sending server receives the *rejection status* and associated *rejection message*. This is not a *Delivery Status Notification* but an actual *SMTP response*.

The result is **E-mail Delivery Certainty**. The sender can always be certain if an e-mail destined for a *PerfectMail™* server was delivered. If it is accepted, it is *always delivered*. If it is rejected the sender *always receives the rejection message.*

Caveat: While we can guarantee the sending server receives the rejection message; we can't control what that server does with it. Most will faithfully pass this rejection message back to the sender; though we have seen instances where this has not happened.

3 Important PerfectMail Setup Notes

The PerfectMail™ Edge Transport Server is a complete *Operating System* and *Application* bundle. PerfectMail includes a highly customized and secured version of Linux. However, knowledge of Linux is not required. All administrative duties can be performed using our *web based user interface*.

WARNING: The Installation CD performs a complete system install. It will erase all existing software on the existing machine. Be sure this is what you want before you install PerfectMail.

PerfectMail acts as an *SMTP relay host*
It makes filter or forward decisions by examining many aspects of an e-mail, including message structure, content, reputation and verification.

PerfectMail does not replace your mail server
PerfectMail filters and forwards e-mail, but is separate from and does not replace your existing mail server. You must run your own mail server; e.g. MS Exchange, Lotus Domino, GroupWise, Sendmail, QMail, etc.

PerfectMail must be your MX Host!
PerfectMail *must* be the first point of contact with the Internet. PerfectMail *must act as a mail exchanger* for your domains (i.e. your DNS MX records will be pointing directly to PerfectMail). If e-mail is relayed through a proxy or intermediate e-mail host, critical information will be lost and PerfectMail's effectiveness will be significantly impaired.

The Firewall must *not* act as an e-mail proxy
Some firewalls can act as e-mail proxies, applying rudimentary e-mail filtering. This option must be disabled. *Only use port forwarding rules to PerfectMail.*

Configure PerfectMail to filter your domains
PerfectMail will only accept traffic for configured e-mail domains. Make sure all your domains are setup using PerfectMail's Web Interface.

Does your mail server do *SMTP Recipient Filtering*?
SMTP Recipient Filtering occurs when your mail server rejects e-mails sent to accounts that *don't exist*. Some mail servers, notably MS Exchange, have this turned off by default. *SMTP Recipient Filtering* is an important method whereby PerfectMail is able to *automatically* validate the existence of an e-mail address. For MS Exchange servers, refer to the section on *Enabling SMTP Recipient Filtering for MS Exchange*.

Relay outgoing e-mail through PerfectMail
Our e-mail reputation engine is a major strength of PerfectMail. This adaptive engine self-trains by watching both in-bound and out-bound e-mail traffic. For maximum effectiveness, PerfectMail needs to see both in-bound and out-bound e-mail. For MS Exchange servers, refer to the section on *Configuring a SmartHost for MS Exchange*.

DNS resolution *must work*!!!
Domain Name Service resolution *must work* for your PerfectMail server to function. PerfectMail *will not accept e-mail from unresolvable domains*! Similarly, the hostname you assign to your PerfectMail server must be fully resolvable in DNS (Example: perfectmail.mydomain.net). This server will be *visible* to the Internet; **an unresolvable hostname name may cause other mail servers to reject *your* e-mail**.

4 Our Philosophy on E-mail Security

We take a different view of e-mail than other anti-spam solutions. Our primary focus is not simply blocking unwanted messages, but allowing legitimate messages through.

An e-mail security product should be safe, secure and reliable. PerfectMail™ is based on the following principles:

1. **Legitimate mail must get through**
   PerfectMail's first goal is to identify and accept legitimate e-mail. Our unique approach ensures we have extremely low false positive ratings. *Business e-mail must get through!*

2. **E-mail servers must be protected**
   E-mail is business-critical. Mail servers are under constant attack from spammers, hackers and other rogue entities. Using PerfectMail as the first point of contact, you effectively insulate your e-mail server from the Internet.

   Using PerfectMail also reduces the amount of traffic that reaches your mail servers. That means a lower load for your servers; and lower costs for your organization. At many of our sites, PerfectMail's *Return on Investment* is high enough to cover cost within a few months.

3. **Spam should be stopped at the edge of your network**
   You have three opportunities to block spam & viruses: at the edge of your network, on your mail server and on the PC Desktop. Malicious e-mail poses a significant risk to your company's infrastructure; it needs to be blocked as soon as possible. PerfectMail acts as an e-mail firewall, protecting your servers and desktops at the edge of your network.

4. **Information is power**
   PerfectMail includes powerful reporting and search tools to show exactly what is happening with your e-mail systems. We provide metrics so you can monitor your infrastructure and make better decisions to ensure you are getting the best return on investment.

5. **Anti-spam solutions should free your users**
   Your anti-spam solution should be accurate and effective, without requiring constant attention from administrators and users. Using adaptive techniques PerfectMail is able to self train, freeing up your administrators and users to be more productive. PerfectMail watches your e-mail traffic and learns who you are, who you know and what you do. Your anti-spam solution should not be more onerous than the problem it's trying to solve.

6. **E-mail addresses belong on your website**
   Make it easy for your customers to contact you: Put your e-mail addresses on your website! While spammers do harvest e-mail addresses from web sites, PerfectMail makes it safe again. We have tools that identify spammers who gather e-mail addresses from your website - and we stop them.

   At PerfectMail we list our e-mail addresses on our website. See if our competitors do that!

7. **Any solution must be compatible with all mail servers**
   PerfectMail acts as an e-mail relay. By filtering e-mail at the protocol level, PerfectMail is compatible with all mail servers, including:

   - ♦ Microsoft Exchange™
   - ♦ Lotus Notes™
   - ♦ Novell GroupWise™

- ♦ Sendmail™
- ♦ and many more

8. **Let you choose your delivery platform**
   PerfectMail gives you the power to choose how to implement your e-mail security solution. We deliver our product in several ways to give you the most flexibility.

   - ♦ *Deploy PerfectMail on your own hardware* - Leverage your existing infrastructure by deploying on: IBM™, Dell™ and HP™; or build your own server.

   - ♦ *Deploy PerfectMail as a Virtual Machine* - Virtualization has many benefits for your organization. PerfectMail is developed and delivered on VMware's virtualization products.

   - ♦ *Order a hosted solution* - Have your e-mail filtered at our Class A data center. We'll give you all the benefits of PerfectMail and we'll take care of the server.

5 PerfectMail Features

5.1 Performance Features

- Simple, 15 minute setup
- Highly efficient code provides extremely fast performance
- Filtering occurs in real time, during message transfer
- Places little strain on our physical server
- Industry leading 99.9+% accuracy, and almost no false positives
- Effective in blocking all sources of spam
- Very fast ROI, within a few weeks for most installations
- Typical message filter time 1-5 seconds
- Typical message processing time 5-100 ms
- Flexible implementation options

5.2 Supported Platforms

- VMware ESXi 5.1, 5.0 and older
- Microsoft Hyper-V
- Citrix XenServer
- Servers from Dell, HP, IBM and others
- Popular Desktop PCs
- Popular white-box PC and Server hardware
- Contact us for hosted solutions or off-site redundancy

5.3 Basic Spam Filters

- Configurable Content Filtering
- Bayesian Content Filtering
- Phishing Analysis
- Sending server analysis
- Outbound E-mail Filtering

5.4 Advanced Spam Filters

- Content Anti-Obfuscation engine
- Word suffix engine
- Spamvertizer Analysis
- Google Safe Browsing filter
- Anti-Spoofing Tools
- Website URL analysis & probing
- Advanced Grey Listing engine
- RX Scanner advanced anti-phishing engine

5.5 Sender Reputation Filters

- Black/White Listing of mail servers, domains and e-mail addresses
- Real-time Block List (RBL) Filters
- Sender Policy Framework (SPF)

- Sender & recipient filter exclusion lists
- Spam Trap functionality

5.6 Anti-virus & Vulnerable Attachment Filters

- Anti-virus scanning of e-mail and attachments
- Zip File Anti-virus scanning
- Vulnerable Attachment filtering
- Zip File Vulnerable Attachment filtering

5.7 Distributed/Co-operative Filtering

- Automated Core & Filter Module updates
- Reported spam analysis turnkey system
- Community Wide Content Filtering of message headers and body
- Spam Profile Engine & Updates

5.8 Web Console Management

- Server status dashboard
- Domain Administration
- E-mail Activity logging
- E-mail Transmission logging
- E-mail Search & Management
- Activity Graphing
- Resource Graphing
- Spam Quarantines
- Full Message Archiving
- E-mail Message Viewing
- E-mail broadcast tool
- Domain based message footers

5.9 End-User Empowerment Tools

- E-mail Activity Reports
- Self-Service Console

5.10 Advanced Web Console

- PerfectMail Message Replay
- Message deletion & shredding
- Custom RBL Configuration

5.11 E-mail Traffic Management

- Domain based Forced Encryption
- Recipient based e-mail routing
- â™ Score & Forwardâ™ Spam Analysis option

5.12 PerfectMail Application Cluster*

- Co-operative application cluster
- Servers work together, presenting a unified front
- Statistical/reputation information duplicated across servers
- Replication of domain/e-mail/spam settings
- Search and view e-mail from any server in one place

5.13 Basic Server Assurance

- Server & Infrastructure Validation system
- Server Configuration Backup tool
- Off-site Server Configuration Backup service

5.14 Advanced Server Assurance

- Active server monitoring and alerts
- Adaptive resource reservation engine to prevent Denial of Service attacks

6 PerfectMail Setup

6.1 Basic Setup

PerfectMail™ is an *Edge Transport Server* based e-mail *filter and relay* solution. Setup your PerfectMail server on the *edge* of your network, just behind your firewall.

Internet <=> Firewall <=> PerfectMail <=> Mail Server

PerfectMail™ is a **live filtering solution**. It filters e-mail in real-time during the actual e-mail exchange.

When an e-mail message arrives at your PerfectMail product, it is subject to our suite of validation and verification tests; many unique to PerfectMail. The result is one of three decisions: *Accepted*, *Tagged* (uncertain), or *Rejected*.

Depending on your configuration the messages may be rejected at your PerfectMail server or simply scored and filtered later.

6.2 Firewall Settings

Port 25 (SMTP) traffic should be forwarded to your PerfectMail product.

It is best to create a one-to-one NAT mapping port 25 on the Internet facing IP address and your PerfectMail product. Problems can arise when the incoming SMTP IP address and the outgoing SMTP IP address do not match. In this situation incoming SMTP traffic is properly configured, however the outgoing SMTP traffic is sent on an unexpected port (usually the default outgoing IP address is used).

When sending e-mail to the Internet remote anti-spam servers will verify the domain name, hostname and reverse address of the sending IP address against your DNS records. Often the DNS records are not configured to support the default outbound IP address.

Anti-spam servers will compare the name reported by the server itself (i.e. the hostname), the address record (A record) from DNS and the reverse DNS record (PTR record). Anti-spam servers will score and possibly even reject messages for discrepencies between these records. This is further complicated by firewall port forwarding issues. The best way is if you have a 1-1 NAT for your e-mail so both incoming and outgoing mail use the same IP number. Failing that the names should all match up on the outgoing side of things.

We strongly recommend updating your firewall to restrict all outgoing SMTP (port 25) traffic. Only PerfectMail and other mail servers should be able to send e-mail directly to the Internet. PC's compromised by viruses, Trojans, etc. may send e-mail directly to the Internet which may result in your entire organization being blacklisted by RBL sites such as Spamhaus. (Especially if you have only one Internet facing IP address.)

Following are two examples of how to configure PerfectMail within your firewalled infrastructure.

6.2.1 Firewall Configuration: Green Zone + Internet

If you have a simple firewall configuration, with your internal network (Green Zone) being protected from the Internet, place your PerfectMail product in the internal network (Green Zone) and configure your firewall to allow the following network traffic.

Incoming Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to Perfectmail for incoming e-mail
443	TCP	HTTPS	Port forward to Perfectmail for remote secure web access (optional)
22	TCP	SSH	Port forward to Perfectmail for technical support (optional)

[Note: Using non-standard ports for support access (i.e. SSH and HTTPS) is acceptable as long as these are port forwarded to the appropriate ports on the PerfectMail server.]

Outgoing Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing
80	TCP	HTTP	For website probing
123	UDP	NTP	For remote Network Time Protocol look-ups
443	TCP	HTTPS	For website probing
43, 4321	TCP	whois, rwhois	For WhoIs queries

6.2.2 Firewall Configuration: Green Zone + DMZ + Internet

For the configuration you described with PM in the DMZ and your Mail Server and DNS in a Green Zone (protected network). The following ports are required for PerfectMail to function:

If you have a firewall configuration that includes a DMZ, with your internal network (Green Zone) being protected from the Internet, place your PerfectMail product in the DMZ network and configure your firewall to allow the following network traffic.

Between Internet and the DMZ - Incoming Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to Perfectmail for incoming e-mail
443	TCP	HTTPS	Port forward to Perfectmail for remote secure web access (optional)
22	TCP	SSH	Port forward to Perfectmail for technical support (optional)

[Note: Using non-standard ports for support access (i.e. SSH and HTTPS) is acceptable as long as these are port forwarded to the appropriate ports on the PerfectMail server.]

Between Internet and the DMZ - Outgoing Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing
80	TCP	HTTP	For website probing
123	UDP	NTP	For remote Network Time Protocol look-ups
443	TCP	HTTPS	For website probing
43, 4321	TCP	whois, rwhois	For WhoIs queries

Between the DMZ and the Green Zone - Incoming Ports, to Green Zone:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to mail server for incoming e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing (unless DNS server is in DMZ)
123	UDP	NTP	For Network Time Protocol (unless time server is in DMZ)

Between the DMZ and the Green Zone - Outgoing Ports, from Green Zone:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
443	TCP	HTTPS	For PerfectMail Web-UI secure access
80	TCP	HTTP	For PerfectMail Web-UI access (optional)

6.3 The PerfectMail Hostname

A server's *hostname is the name that it knows itself as. This is different than naming in DNS or any other mechanism. It is the locally defined name.*

Your PerfectMail™ product **must** have a *resolvable, fully qualified hostname*; e.g. `perfectmail.mydomain.com`. There **must** be a domain portion to the *hostname* of your PerfectMail server.

This *hostname* must be resolvable in DNS. Mail servers will look-up server names in DNS as a validation mechanism. Not having a resolvable *hostname* can cause problems.

If this is not possible to use resolvable DNS names you can use the `.localdomain` domain; e.g. `perfectmail.localdomain`.

Your PerfectMail *hostname* must also be unique. Often, mail servers will refuse to relay e-mail through mail servers with the same *hostname*. This is done to prevent endless e-mail delivery loops.

6.4 DNS and Mail Servers

Note: This is not a tutorial on DNS and gives no guidance on how to make DNS changes.

Mail servers do quite a bit of validation to help stop spam; hostname validation being one of them. There are three items that are commonly cross validated, and may result in message rejection:

- Machine hostname (as it is recorded on the mail host)
- DNS A record
- DNS PTR record

Mail servers share their locally defined hostnames with each other (e.g. perfectmail.yourdomain.com). The SMTP exchange starts with a "hello" phrase where this information is passed. The name given may then be validated against DNS A records and PTR records. Best practice is to ensure that DNS records with the same name exist for the hostname of your mail server.

Something else to note: Mail servers will not deliver e-mail to servers that have the same locally defined **hostname** as itself. It's a validation check to prevent endless e-mail loops. Note, the hostname is the name the server uses to identify itself locally; regardless of what DNS records (or any other records) say. **If your back-end mail server has the same hostname as your PerfectMail server, e-mail will not flow.**

DNS allows for multiple entries in it's resolution scheme for both A and PTR records, so you can create additional records to ensure mail servers can fully validate the perfectmail server, without affecting other records.

For example, here are DNS records for a fictional PM server, who's fully qualified hostname is `perfectmail.somedomain.com`:

```
perfectmail.somedomain.com.          IN A     216.85.75.194

194.75.85.216.in-addr.arpa.          IN PTR   perfectmail.somedomain.com.
```

6.5 Implementation Options

PerfectMail™ is an *edge based* e-mail relay and filtering solution. This gives it the flexibility to work with all SMTP based e-mail servers and meet most implementation requirements.

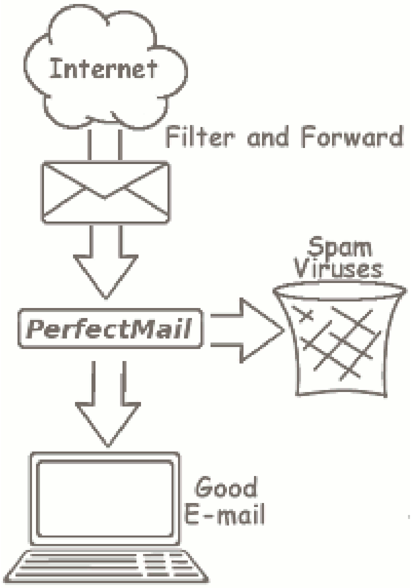
There are two basic implementation schemes: *Filter & Forward* and *Score & Forward*. In both schemes PerfectMail analyzes and scores incoming e-mail for spam. The difference is when the actual filtering takes place.

6.5.1 Filter & Forward Implementation

Filter & Forward is the simplest implementation method, requiring no changes to your *client PC's*. In this method the PerfectMail™ server scores each e-mail and filters out spam. Only the filtered e-mail is forwarded to your mail server; and client PC's.

In this implementation:

- PerfectMail analyzes the message
- PerfectMail discards spam and viruses
- PerfectMail forwards good e-mail
- All forwarded e-mail goes into your in-box
- Administrators release messages as needed
- Administrators have better understanding of e-mail issues
- Reduced e-mail traffic as spam is filtered



Filter settings that allow you to implement *filter & forward* are located in the web interface under "Filtering > Filter Settings".

6.5.2 Score & Forward Implementation

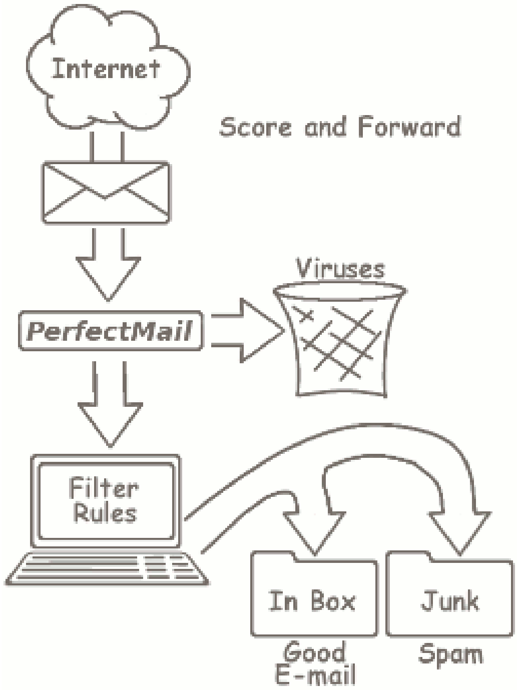
Score & Forward is a more complicated solution, but one that gives your users more control over their e-mail. In this method the PerfectMail™ server scores each e-mail and adds custom e-mail headers to signify the score or disposition of the message. Your mail server or e-mail client (e.g. Microsoft Outlook) uses these headers to filter the e-mail.

In this implementation:

- PerfectMail analyzes the message
- PerfectMail discards viruses
- PerfectMail scores and marks messages based on content
- All e-mail is forwarded to your computer
- Mail client separates messages based on filter rules; sorting into in-box or junk folders
- Users can recover filtered e-mail quickly by checking their junk folder
- Greatly reduced administrator interaction

The available e-mail headers are as follows:

- **X-PM-Score: 15** - Gives the spam score of the e-mail numerically
- **X-Spam-Level:** ***** - Gives a graphic representation of the spam score. Each '*' represents 5 points of the spam score.
- **X-Spam-Flag: YES** - Gives a definitive spam decision based on your thresholds



Filter settings that allow you to implement *filter & forward* are located in the web interface under "Filters > Filter Settings".

Your e-mail clients or server need to have *filters* enabled to filter spam based on these mail headers. Instructions for enabling filtering for many popular e-mail clients are in the *reference* section of this document.

6.6 Relaying E-mail Through PerfectMail

PerfectMail™ needs to see both *incoming* and *outgoing* e-mail traffic in order to make effective and consistent filtering decisions. PerfectMail watches the two way traffic between your local e-mail users and their remote e-mail peers. This two-way traffic allows PerfectMail to build an activity database to implicitly white-list your known e-mail peers.

Configure your mail servers to use the PerfectMail server as a *Smart Host* for e-mail. Instructions for this are specific to your mail server, however we have included some notes on this topic in the reference notes of this document.

6.7 Recipient Filtering

Recipient Filtering is a process where e-mail destined to addresses not hosted on your mail server are rejected during transmission. This is an important tool in reducing the volume of spam serviced by your mail server.

PerfectMail™ performs *recipient filtering* on incoming e-mail based on it's list of known e-mail addresses. Under normal operation, PerfectMail uses a progressive scheme that selectively queries your mail server to build a local database of known e-mail addresses.

To support this functionality, it is important that *recipient filtering* is enabled on your mail server. There are notes in the reference section for enabling this in Microsoft Exchange™ (which has this feature disabled by default.) If *recipient filtering* is disabled PerfectMail will receive responses that make it look like all e-mail addresses are valid on your mail server.

If *recipient filtering* cannot be enabled on your mail server, you need to disable this feature in PerfectMail's *Domain Admin* pages.

7 Active Directory

Active Directory (AD) can be a problem for third party tools. AD integration/configuration is not necessarily consistent and we've had reports from third party vendors who are very experienced with AD but still encounter quirky behavior; AD can require a bit of finesse. However, with *SMTP Recipient Filtering* enabled we simply do not need AD as we can authenticate e-mail addresses directly with Exchange.

By default Exchange will accept all e-mail, regardless of the recipient. SMTP Recipient Filtering is a feature where Exchange will only accept e-mail that it can either route or deliver. PerfectMail uses an algorithm to interactively query Exchange using the SMTP protocol to validate e-mail addresses rather than relying on AD. The implementation is very straightforward and works flawlessly.

7.1 Microsoft Outlook Junk E-mail Reporting Add-in

Microsoft™ has provided an add-in for Outlook™ to allow you to report your spam as Junk using just one click. Using the Junk E-mail Reporting Add-in, PerfectMail is able to identify and immediately train your spam on your local PerfectMail server without you having to use the PerfectMail console.

The Junk E-mail Reporting feature integrates into Outlook 2003, 2007, 2010 and 2013.

Install the Junk Email Reporting Add-in...

Download and run the Windows Installer .msi file to have the Junk E-mail Reporting Add-In Setup Wizard. You must have administrator privileges to run the Setup Wizard. You must also be using the following:

- Operating System: Windows 8, Windows Server 2012, Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista SP2, Windows 2003 SP2, or Windows XP SP3;
- Micrsoft Outlook: Office Outlook 2013, Outlook 2010, or Outlook 2007 (Service Pack 2 or higher);
- Microsoft Office Primary Interop Assemblies (To download go to the Microsoft Download Center);
- Microsoft .NET Framework Version 2.0.

Setup:

1. On your computer, close Microsoft Office Outlook if it is open.
2. Go to the Microsoft Download Center page for the Microsoft Junk E-mail Reporting Add-In for Microsoft Outlook http://go.microsoft.com/fwlink/?LinkID=147248 and download the .msi file.
3. Double-click the .msi file.
4. On the Welcome to Microsoft Junk Email Reporting Add-in Setup page, click Next.
5. Review the license agreement, and then click I accept the terms in the License Agreement if you agree to the terms of installation and click Next to continue.
6. When the wizard is complete, click Finish.
7. Start Microsoft Office Outlook.
8. Confirm the add-in had been successfully added by looking for the Report Junk button on your Outlook taskbar.

To report spam:

1. Select the junk email (spam) messages in your Inbox (up to 10 spam messages at a time).
2. Click the Report Junk button.

More information on Junk E-mail Reporting:

- With the Junk E-mail Reporting Tool you can report a message with only one click.
- PerfectMail is able to identify and immediately train spam submitted using Junk E-mail Reporting.
- Submitted messages are forwarded to PerfectMail for analysis and new PerfectMail signatures are generated daily.
- You can train up to 10 messages at a time.
- Outlookâ™ s Junk E-mail local filter does not learn from your marking messages as Junk.
- Outlookâ™ s Junk E-mail local filter does not learn from your moving them into the Junk E-mail folder.
- Outlookâ™ s Junk E-mail filter definitions are updated via Microsoft Update on an almost monthly basis.
- Submitting a junk E-mail doesn't guarantee that it will be caught the next time.
- By submitting Junk E-mail for analysis you can help train your filters and reduce the spam you receive.
- The Junk E-mail Reporting feature integrates with Outlook 2003, 2007, 2010 and 2013.

For more information refert to Microsoft Technet article:
https://technet.microsoft.com/en-us/library/jj723139%28v=exchg.150%29.aspx

8 PerfectMail Web Admin Interface

PerfectMail™ provides a rich *Web-based User Interface* (Web-UI) on a simple 2-level *ring menu* to make administration easy. We use the following convention to reference these web pages:
"MenuName > AdminPage"; for example: "E-mail > Transmission Log".

Each page of the *Web-UI* has a **Help?** link located at the top-right corner of the page where all of the following information can be accessed by the **Help?** link.

The user interface is *highly click-able* to make navigation simple and intuitive. Click-able links are colored blue.

8.1 The Dashboard

The *dashboard* presents a summarized view of your PerfectMail™ product. There are many *links* to configuration and status pages. With the *dashboard* you can quickly view:

- the state of the running services,
- anti-virus details,
- the server load,
- statistics from the last 24 hours,
- the size of the message queue,
- license information, and
- announcements from PerfectMail.

From the *dashboard* you can stop/start both the *anti-spam engine* and *mail transport agents*.

You can force PerfectMail to check for new *virus signatures* (done automatically every 10 minutes).

There are also links to *shutdown* or *reboot* the server itself.

8.1.1 How to Start and Stop PerfectMail

The PerfectMail™ anti-spam service will start automatically when your PerfectMail server boots.

There are several ways to shutdown your PerfectMail™ server:

1. Login to the *Web Interface* and click the "shutdown" link on the dashboard,
2. Login to the system console as "root" and issue the "shutdown" command,
3. For a physical server, hit the power button once, or
4. For a virtual server, click the appropriate link to shutdown the Guest OS.

8.2 The E-mail Menu

This menu contains query pages showing actual e-mail activity and logging information. Each query page on this menu presents different entry points into the *PerfectMail™ e-mail activity search engine*.

8.3 The Filters Menu

The *Filters Menu* holds pages used to configure how your PerfectMail™ product filters e-mail.

8.4 The Reports Menu

The *Reports Menu* presents a collection of reports giving information for both server activity, statistics; and details on specific e-mail addresses, server addresses and messages.

This area of the Web-UI is under active development. More reports will be added in future releases. Also, we will soon add functionality to allow you to schedule and e-mail your reports.

8.5 The Domain Admin Menu

This menu contains pages for managing the settings for protected domains, e-mail addresses and other relaying servers.

8.6 The Server Admin Menu

This menu contains pages for managing the configuration of your server; including networking, access and licensing.

8.7 The Tools Menu

This menu contains administrator tools for server and connectivity diagnostics; as well as other administrative tools.

9 Basic Server Management

9.1 Server Settings

9.1.1 Server Admin > Network

Network settings configuration.

Use this screen to configure your servers network settings. Be aware that changing network settings may make the Web-UI unavailable, so use caution when making changes. Also note that *DNS Settings* can have a critical effect in the performance of this server. Refer to the *DNS Servers* below for more information.

DNS Settings and the Hostname:
It is important to maintain consistency between the *hostname* of this server and the DNS records referring to it. The hostname of your PerfectMail™ server is very important. Remote mail servers will attempt to verify this hostname against DNS records. If the hostname is not resolvable, most mail servers will reject any e-mail your server sends. Specifically anti-spam servers will check that:

- The *hostname* of your PerfectMail server is fully qualified and resolvable. (I.e. your domain name must be a part of the hostname and it must be a real, resolvable domain name. If this is not possible use the ".localdomain" domain.)
- There is an *A* record in DNS that resolves to the advertised IP address of this server.
- There is a *PTR* record in DNS resolving to the advertised IP address of your server.
- Anti-spam servers may check that the hostnames referred to by PerfectMail (the A and PTR records) all match.
- You should create a TXT record in DNS containing an SPF policy for each e-mail domain you host.

(Note: If the concepts above are new to you or if you have questions, contact our support staff for assistance.)

Host name:
The fully qualified hostname of this server. (e.g. myhost.mydomain.com) This should always be populated and fully qualified. **If the hostname is not fully qualified, your PerfectMail server will likely hang!!!**

Network Interface:
Choose either a *dynamic* or *static* configuration. As this is a mail server we strongly recommend a static configuration (in keeping with the hostname issues discussed above.) The *IP Address*, *Netmask*, and *Default Gateway* use standard 4-octet formatted IP addresses. Example:

```
     IP Address: 192.168.0.100
        Netmask: 255.255.255.0
Default Gateway: 192.168.0.1
```

DNS Servers:
IMPORTANT: *DNS resolution is a requirement for the proper operation of your PerfectMail server. Failure to perform DNS requests will result in a rejection of all e-mail delivery requests.* Enter the IP Addresses of up to 3 *DNS servers*, using the standard 4-octet formatting described above.

Alternate Ports:
If you have statically assigned your network configuration, you can configure alternate ports for receiving ssh or www traffic. This may be used as a workaround if you want to use non-standard ports for these services on the internet but your firewall doesn't give the option of port-forwarding from one port to another.

9.1.2 Server Admin > Time

Change the system time and location (time zone) and configure *Network Time Protocol (NTP)* settings using this page.

NTP is a protocol designed to synchronize the clocks of computers over a network. NTP uses UDP on port 123; so this port must be opened on your firewall. No information about time zones or daylight saving time is transmitted; this information must be initially set locally using the Date/Time/Timezone fields on this page.

For *virtualized* environments, the *Network Time Protocol* should be disabled, so it does not conflict with any virtualization tools in place.

9.1.2.1 Clock Drift

Clock Drift is when your system clock gradually drifts away from the current time. This may sometimes occur with older systems and is an inherent problem with virtualized environments. For a purely hardware based environment the NTP service should remedy the problem. Just ensure the NTP protocol (*port 123 UDP*) is not blocked by your firewall.

For *virtualized* environments running NTP can be problematic and will likely result in clock drift. The virtualization tools are constantly adjusting the system clock as a side effect of virtualization; which conflicts with NTP. Turn off NTP for virtualized environments.

If you are experiencing clock drift it's best to experiment with these settings. If it's possible, select NTP servers within your organization or that are being used on other servers within your organization.

9.1.3 Server Admin > Certificate

This Server Certificate and Key are used by both the PerfectMail e-mail and web services. Use this page to *generate a self-signed certificate*, or to apply your own certificate information.

9.1.3.1 What is SSL?

Secure Sockets Layer (SSL) is an encrypted protocol designed to enable applications to transmit information back and forth securely. Applications that use the Secure Sockets Layer protocol inherently know how to give and receive encryption keys with other applications, as well as how to encrypt and decrypt data sent between the two.

Applications configured to run SSL including web browsers, email and other programs requiring secure data transmission.

To establish a secure SSL connection, PerfectMail must first have an encryption key. This can either be a *Self Signed Certificate* or a certificate assigned by a Certification Authority.

9.1.3.2 Generating a Self-Signed Certificate

The *Self-Signed* certificate is generated using information from both the *Licensing* page and the hostname from the *Network* page, so please ensure this information is correct. Use the following proceedure:

1. Review/update your company licensing information on the Licensing page (Server Admin > Licensing).
2. Review/update your *hostname* on the Network page (Server Admin > Network).
3. Click the *Generate Self Signed Certificate* button on the Certificate page (Server Admin > Certificate).

9.1.3.3 Creating a Certificate Signing Request

The *Certificate Signing Request* certificate is generated using information from both the *Licensing* page and the hostname from the *Network* page, so please ensure this information is correct.

9.1.3.4 Changing the Server Key

You may want to change the *Server Key* to take advantage of an existing certificate, including wildcard certificates. If you need to change the *Server Key* this needs to be performed as a separate step from other activities using the following procedure:

1. Update the *Server Key* content on the Server Key tab.
2. Click the *Update* button.
3. Changing the *Server Key* will automatically generate a new Self-Signed Certificate. After this step you can make changes to any other certificate fields/tabs as required.

9.1.3.5 Applying a Certificate to your Server

Your PerfectMail server only supports the standard x509 certificates in PEM format. PEM formatted certificates wrap then content with Begin/End Certificate markers as follows:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

You may find different filename extentions used on these files. Commonly you will find the following:

- .crt - Common Certificate extension (can be ASCII PEM or binary DER)
- .cer - Alternate form of .crt (Popular with Microsoft products)
- .pem - Pem formatted file

Installing your certificate..

1. If you need to update your *Server Key* follow the procedure mentioned above before continuing.
2. Your *Certificate Authority* will issue you with a PEM formatted Certificate or a Wildcard Certificate (.crt). Copy and past the content of this file into the *Server Certificate* tab of the Certificate page (Server Admin > Certificate).
3. Your *Certificate Authority* will also issue you with a root CA Certificate (.crt) or Intermediate Certificate (.crt). They may send you multiple certificates. Copy and past the content of one of these files into the *CA Certificate* tab of the Certificate page (Server Admin > Certificate).
4. Click the *Update* button at the bottom of the web page. You may have to reboot or reconnect your web browser to PerfectMail.

9.2 Server Access & Licensing

9.2.1 Server Admin > Users

PerfectMail™ User Interface Accounts.

This page allows you to configure user access to the User Interface. Click on a *user name* to edit or remove existing users or click *Create User* to create a new user. User names should be relatively short (about 8 characters) and must not contain spaces or punctuation.

It's important to ensure you fill out all of the fields on this form. The user's e-mail name and e-mail address may be used for sending reports, e-mail blasting and reporting issues with your PerfectMail server.

Permissions:
There are three account types:

- **Administrator** - Administrators have full access to all aspects of the user interface.
- **User** - Users are able to view information and perform queries, but are generally unable to make changes. You can selectively assign server wide permissions to each user as is needed.
- **Web Service** - The *web service* interface allows external systems to interface with your PerfectMail server. Web services generally have very restricted rights. For more information on integrating servers using *web services*, contact our support staff.

Login Restriction:
You can restrict access to this *User Interface* to specific IP addresses or ranges.
Examples:

```
Unrestricted access...

IP Address: 0.0.0.0
   Netmask: 0.0.0.0

Restricted access via a single IP address...

IP Address: 192.168.100.13
   Netmask: 255.255.255.255

Restricted access via an IP address range...

IP Address: 192.168.100.0
   Netmask: 255.255.255.0
```

9.2.2 Server Admin > License

Server registration and licensing page.

It is important that you record accurate contact information and register your PerfectMail™ product. Information from this page will be used to generate a self-signed certificate for your PerfectMail™ product. Contact information from this page will be used by your server to contact you if there is ever a problem with your server. You may be contacted by PerfectMail staff or the server may automatically send you a notification e-mail if it finds a problem.

The *license number* and *activation code* are provided by PerfectMail staff. When your server is licensed you may need to provide your *Machine ID*.

NOTE: You must read and accept the *license agreement* available via a link at the bottom of this page. Otherwise, your PerfectMail server will run in demo mode and not filter spam.

If you have any questions, contact our PerfectMail support staff.

9.2.3 Server Admin > Server Settings

This page controls various server related settings for your PerfectMail™ server. The settings control how e-mail messages are stored and viewed, what reporting features are available and how the server can be accessed.

Security Settings:

- **Show graphs on login screen** - Display activity graphs on the login page. This may be a convenient option to display general statistics without requiring authentication.
- **Allow only secure connections** - Accept only secure http connections to the web interface, i.e. https://
- **Enable message store** - Normally PerfectMail will store up to two weeks of messages. Un-checking this box will *turn off message storage*.
- **Encrypt message store** - Causes PerfectMail to use a simple encryption technique to secure message content on the disk. It prevents casual browsing of content from anyone who may gain access to the raw message files, but does not prevent validated users from viewing message content. Unless this is a concern, we recommend turning off this feature to avoid system overhead.
- **Allow message viewing** - Allow message content viewing in the web interface. Note: users with Administrator access can always turn this setting on or off.

Support Settings:

- **Automatic server updates** - When an update becomes available, automatically update this server.
- **Enable Server Validation** - Send notification e-mails to the PerfectMail administrator if there is a serious configuration issue with this server.
- **Remote Config Backup** - Periodically, your server will forward a copy of it's configuration to our backup server. If you suffer a catastrophic failure, we can quickly restore your server. No message content is ever sent. We highly recommend turning on this feature.
- **Statistical Reporting** - This gives PerfectMail staff clear & early warning of developing spam trends. Only statistical information is sent. No message content is ever sent. We highly recommend turning on this feature.
- **Server Monitoring** - Active and passive monitoring of your server. Monitoring the health of your server ensures early notification of any problems. We highly recommend turning on this feature.
- **PerfectMail support access** - If there is an issue on your server, selecting this feature gives permission for our staff to proactively attend to it. Disabling this feature will disable all support staff access to your server.

Activity Report:

E-mail Activity Reports provide your users with direct access to their e-mail, with options to release quanrantined messages, resend accepted messages and report any spam that has gotten past the filters.

Manage global report settings here. Manage user specific settings using the Domain Administration page. Each domain has a list of users whom you can specify individual settings.

For weekly and monthly activity reports, the report will be sent on the first report hour selected on this page. For example, for settings of 08:00 and Monday a weekly report would be sent at 08:00 each Monday; and a monthly report would be sent at 08:00 on the first Monday of the month.

For Action Links to work in the report you must ensure the Web URL of this server is specified as the users will see it.

The *Activity Report Setup Wizard* will guide you step-by-step through the setup of these features.

9.3 Other Server Settings

9.3.1 Server Admin > Archive

Logging, statistics, and message storage database settings.

PerfectMail™ functions best when the volume of stored messages is kept relatively small; about two weeks of data. However, this can be increased as needed to provide archiving functionality. (In the near future this functionality will be increased to include full text search and retrieval.)

Keep statistics for longer periods. At least 90 days of log data should be kept; to a maximum of 365 days.

The data store is trimmed on a daily basis. It is important to ensure enough free disk space exists to support one day of e-mail activity on your server. Please ensure there is a generous about of free system disk. Message content takes up lots of room, while log content is much less spacious.

WARNING: If the file-system fills to 100% your PerfectMail server will **stop functioning.**

9.3.2 Server Admin > Backup

PerfectMail™ Server Configuration Backups

Use this interface to create backups of your servers configuration. The backup consists of:

- basic server settings,
- network settings,
- domain configuration settings,
- mail filtering settings,
- black/white lists, and
- other settings.

But does not include e-mail message history or e-mail content.

Note: License information will not be backed up. License activation codes are tied to the machine id of your server; they can not be transferred to other servers. Rebuilding your server may also invalidate the activation code. If you have any issues with licensing or activation contact our support staff.

Create New Backups periodically to ensure you can recover from system failures. It's a good idea to enter a description for each backup.

Download your backups and keep them someplace safe. To download a backup, click on the backup's date stamp.

If needed you can *upload a backup* using this page as well. The system will verify that this is a proper backup file and ensure that it's contents are sound.

9.3.2.1 Restoring Backups

To *restore* a configuration, click the restore link beside the desired configuration. Two types of restoration are available:

- *Restore Settings* - Restore domain configuration and spam filter settings, but **does not restore server network settings**.
- *Restore Server* - Restore all server settings **including server network configuration**.

In either case, license settings are not restored.

To *restore* a configuration, click the restore link beside the desired configuration.

9.3.3 Diagnostic Tools

What network diagnostic tools does PerfectMail provide?

PerfectMail™ provides a number of tools on its web interface (on the "Tools" menu) to provide administrators with the means of easily diagnosing network problems. The following tools are available:

- **DNS Look-up** - Used to perform DNS look-ups;
- **Ping** - Used to test network connectivity between PerfectMail and another network device;
- **TraceRoute** - Used to trace the network route between PerfectMail and another network device;
- **WhoIs** - Used to look-up human readable information about an Internet domain name;
- **SMTP Test** - Used to diagnose low level SMTP protocol exchanges between PerfectMail and another mail server.

Additionally, PerfectMail performs periodic diagnostics of its configuration and connectivity to local infrastructure and the Internet. PerfectMail displays the health of its DNS configuration, Network Status and Mail Server Status on the Dashboard. The detailed results of these diagnostic tests are available in the Server Status Report, "Reports > Server Status".

10 Managing Domains & Relays

10.1 Filtering and Relaying

PerfectMail™ works as a server based e-mail *filter and relay* solution. It watches and filters both *incoming* and *outgoing* e-mail traffic. For PerfectMail to work correctly it needs to know which e-mail domains to manage and which servers to relay e-mail to and from.

Relay Servers are known e-mail servers that are allowed to relay e-mail through your PerfectMail™ server.

Incoming Relay Servers, such as secondary mail exchangers do not receive any server checks (e.g. RBL, SPF and other server based checks), but e-mail messages originating from these servers are still processed using most other anti-spam tests.

Outgoing Relay Servers are considered known and trusted. No filtering will be performed on e-mail originating from these servers.

Both *incoming* and *outgoing* relay servers are defined using the "Domain > Relay Servers" page of the admin interface.

Back-end Mail Servers are the mail servers PerfectMail is protecting. When PerfectMail receives an e-mail it checks it against the list of *domains*. If it is a protected domain it analysis the e-mail for spam and forwards clean messages to the appropriate mail server. This *back-end mail server* is also expected to send e-mail through PerfectMail as a *SmartHost*.

All relay servers must either be defined in the *Domains* or *Relays* configurations.

10.1.1 Domain Admin > Domains

Configuring Domains Protected by PerfectMail™

All e-mail domains you wish to protect with PerfectMail™ *must be listed* in the Domains table. The number of domains that may be administered at any one time is dependent on which edition you are using. Incoming e-mail to any domain *not listed in the Domains table will be rejected*. The only exceptions to this are for the servers listed as *Outgoing Relay Servers*.

This page provides summary information for all of the domains being protected by PerfectMail™. The table is organized as follows:

- **Domains:** The number of administered domains and the name of each domain;
- **Tag:** The spam score at which an e-mail is suspected of being spam. An e-mail with a spam score in the range of Tag <= spam score < Reject results in the text [SPAM?] being prepended to the subject line. See the Filter Settings section below for more details;
- **Reject:** The level at which the e-mail is judged to be spam, this results in the message being quarantined, rejected, or refused;
- **Mail Host:** The IP address of the internal mail host, typically this is not the same as the Mail Exchanger IP address;
- **Status:** The status of the e-mail domain (e.g. OK, Filtering off).

From this page, you can:

- **Add Domain(s):** By clicking on the *Create New Domains* button. When adding domains enter one domain per line in the *domains* box. Each domain will get the settings defined on the Mail Host and Filter Settings' tabs.
- **Modify Domain Settings:** You can selected domains to be modified in one of two ways. You can left-click on the domain or you can check off multiple check boxes and click "Update Selected Domains" to make uniform changes to all of the selected domains.
- **Delete Domain(s):** One or more domains can be deleted by checking their check-box and clicking the *Delete Selected Domains* button.

Use the the Domains table **Search** field to display a subset of all of your managed e-mail domains. Then you can select them all and update the settings for all similar domains at once instead of having to apply the same settings to each domain one at a time. The text you enter in the Search field is used to match domain names and mail host IP addresses.

10.1.1.1 Domain Maintenance - Mail Host Tab

Delivery Hosts:
The *Internal Mail Host* holds the *IP address* of the internal mail server that mail for this domain should be delivered to.

E-mail Validation:

- **SMTP Recipient Filtering** - A validation technique where PerfectMail queries an internal mail server for e-mail addresses. If your mail server accepts all e-mail addresses your PerfectMail™ product will become swamped with bogus information. If this is the case, *turn off SMTP Validation*
- **Locally Defined Addresses** - PerfectMail always validates e-mail addresses against the *Valid Addresses* table.
- **Reject Unknown Addresses** - Reject any e-mail where the recipient address has not been validated using one of the above methods.

NOTE: You must know whether your mail server is giving proper SMTP recipient filtering responses. For example, Microsoft Exchange servers often accept all messages. If this is the case, please turn on SMTP recipient filtering. For Microsoft Exchange systems see *Enabling Recipient Filtering for MS Exchange* in this manual. If SMTP recipient filtering isn't configured properly and you aren't populating the *Valid Addresses* table, then you *must* turn off *Reject non-validated email*.

If you aren't sure if your mail server is giving proper SMTP recipient filter responses, contact PerfectMail support for assistance.

10.1.1.2 Domain Maintenance - Filter Settings Tab

Basic Settings:

- **Filter** - Perform anti-spam filtering on this domain. If filtering is turned off, or if your license is expired e-mail will still be delivered through your server.

Tag and Reject Thresholds:
When an e-mail message arrives at your PerfectMail server it is subject to numerous validation and verification tests. The cumulative value of these tests becomes the *spam score* of the message. The base score is "0". The more *spammy* a message is, the higher the *spam score*. The message is then treated in one of three ways:

ACCEPT
Messages scoring below the *tag threshold* are accepted. (Accept)
REJECT

Messages scoring over the *reject threshold* are rejected (Content-Block). A value **26** or slightly higher is a good starting point. A long term default for **Reject** would be **22**.

TAG

Messages scoring between the *tag* and *reject* thresholds have an uncertain disposition. We "Tag" the subject line of the message [SPAM?] and deliver it to the recipient. The user does not need to check a quarantine. An initial value of **16** or slightly higher is a good starting point and will ensure that very few legitimate messages are tagged. A long term default for **Tag** would be **12**.

Reject Dangerous Attachments:
Enable the blocking of *dangerous attachments* to this domain. Dangerous attachments are defined in the "Filters > Filter Settings Menu". The list of attachments generally consists of things like .exe, .com, .bat, etc.

Only Accept TLS Connections:
For this domain, only accept incoming connections where the transport is encrypted via SSL/TLS.

10.1.1.3 Domain Maintenance - Standard Mail Trailer Tab

Standard Message Trailer/Disclaimer:
Create a standard outgoing message trailer/disclaimer for this domain. This disclaimer will be appended to all outgoing e-mails from this domain.

10.1.2 Domain Admin > Relay Servers

Relay Servers are known e-mail servers that are allowed to relay e-mail through your PerfectMail™ server.

Incoming Relay Servers, such as secondary mail exchangers, do not receive any server checks (RBL and SPF for instance). The e-mail messages originating from these servers are still filtered using all of the non-server anti-spam tests.

Outgoing Relay Servers are considered known and trusted, just like your mail server. No filtering will be performed on e-mail originating from these servers.

Anti-virus checking is performed on all e-mail for Incoming and Outgoing relay servers.

Entries in this table use the following format:

- **IP Address:** *X.X.X.X* or *X.X.X.X/Y* - to specify an IP address or net block.

Example:

```
192.168.0.7
10.3.16.1/32
207.219.44.0/24
```

10.1.3 Domain Admin > Force Encrypt

Force Encrypted Communication with External Domains.

Normal E-Mail Behaviour
Before an e-mail message is actually sent between two domains, the sending server (domain) contacts the receiving server to begin a negotiation. Part of that negotiation is how the message will be sent by the sender to the receiver. The two domains start by trying to negotiate an encrypted connection using SSL. If the two domains fail to negotiate

an encrypted connection, they will negotiate a *plain text* connection. The e-mail is sent once an encrypted or plain text connection has been negotiated.

Force Encrypt's Effect

The behaviour between PerfectMail™ and domains listed in the Force Encrypt table begin in the same manner as described in the above section. The difference occurs when PerfectMail™ and the external domain fail to negotiate an encrypted connection. At this point PerfectMail™ will not allow a *plain text* connection to be negotiated. The sender will receive a response message indicating that the message could not be sent.

When To Use

It is possible for third parties to "listen in" on traffic between e-mail servers (domains). An e-mail that is sent in *plain text* provides no privacy for the sender or the receiver. If you have particularly sensitive data (e.g. financial or personal) that is regularly exchanged with a particular domain, you should have PerfectMail™ enforce an encrypted connection for all e-mail transmissions concerning that domain.

How To Use

To *force encrypt* e-mail traffic with an external domain; enter the domain, one entry per line, in the Force Encrypt Table. You may use domain names, IP addresses, and net blocks. Here are some example entries to the Force Encrypt Table:

their_domain.com
204.10.243.26
207.219.44.0/24

At this time PerfectMail™ does not provide support for Internet Protocol version 6 (IPv6) addresses.

11 Filtering E-mail

11.1 Spam is a Moving Target

Part of the nature of spam is that it comes in waves or surges. The spammers are developing new techniques to both strike a reaction with their "targets" and avoid blocking by anti-spam systems. Having a sudden switch in the type of spam you may receive is very common; occurring when your e-mail address gets put on a list of potential targets.

It's very difficult to stop e-mail based on the presence of one or two words, especially if those words may occur in non-spam messages. It's almost impossible to have a computer make that decision. Our adaptive engine looks for trends in the content it receives. The engine examines the statistical likelihood a message is spam. This does have an effect on the spam that gets through, but that effect is not 100%.

11.2 Scoring Spam

Each e-mail is assigned a numerical *score*, generated by our anti-spam engine. The initial score of a message is "0". We use many techniques to scan each message to see how "spammy" it is. The cumulative value of each test becomes the spam *score* of the message.

We have two thresholds, defined for each domain, that determine what happens to each message. The more *spammy* a message is, the higher the score. If the score reaches the *tag threshold* the e-mail will be tagged. If the score reaches the *reject threshold* the e-mail will be rejected.

Similarly, we look for evidence that the message is legitimate, reducing the spam score. Thus, the *spam score* can be a positive or negative number. The higher the number (positive) the more spammy it is; the lower the number (negative) the less spammy.

Tests that result in a high impact are examined first: virus scanning, black/white listing, sender history, etc. These tests take precedence; they can set the message result by themselves and may cause other tests to be skipped.

Some very expensive tests can get very good information about the sender; but they are done last and only if the test can change the disposition of the message.

We examine the traffic patterns between the sender and recipient. For legitimate senders, as their traffic history accumulates, their *spam scores* drop until the sender becomes *implicitly white listed*. This ensures their messages will never be blocked in error.

If the message is not *accepted* or *rejected* by the high impact tests, it is then classified based on it's spam score and the Tag and Reject thresholds defined for the recipient.

PerfectMail™ uses three categories when scoring messages:

Accept
: After being thoroughly scrutinized, the message was deemed wanted and is immediately forwarded to the intended recipient(s).

Reject
: Messages that are rejected typically contain any of: unwanted content, obfuscated text, misleading or inaccurate e-mail header and/or envelope information, references to spam-friendly networks or other criteria that strongly indicates spam. As a result, PerfectMail™ refuses the message with an appropriate explanation to the sender. Reject messages are customizable so that in the unlikely chance the message was rejected in error, the sender can contact you by other means (phone).

Tag

PerfectMail™ tags messages that score above the Accept threshold but below the Reject threshold. We "Tag" the subject line of the message [SPAM?] and deliver it to the recipient. The user does not need to check a separate quarantine. Typically less than 1% of all messages are tagged.

11.2.1 Tagged Messages

Tagged messages are message that are of indeterminate disposition; they have a score that puts them on the borderline between legitimate e-mail and spam. They are *tagged* with a text based note (by default it is [SPAM?]) on the subject line, but otherwise is delivered normally. (You can turn off the actual subject line tagging in *Filter Settings*, if needed.) Messages that are tagged and are also from unknown servers, seen for the first time, may be *grey listed*.

Grey listing is a process where the server reports that it is temporarily unable to service the e-mail. The sending server receives this notification while attempting the mail exchange. The normal behaviour of mail servers is to try sending the message again after a short delay (usually 5 or 10 minutes). After 3 minutes or 3 attempts to deliver a "grey listed" message, that message will be accepted.

Note: Messages containing viruses, unwanted file attachments, or known Phishing (fraudulent) messages are always rejected.

11.2.2 Message Thresholds

Administrators must assign default values for the **Tag** and **Reject** thresholds for each domain protected by PerfectMail™. It is common practice to start with higher values, to ensure no false positives (legitimate mail rejected as unwanted) and then adjust values down over time. Higher initial values will allow some amount of unwanted e-mail (spam) to sneak in under the **Tag** and **Reject** scores. Determining and setting safe, long-term values for Tag and Reject can stop unwanted e-mail activity.

PerfectMail's reputation system will learn your users and their peers within a few days to a few weeks of service. Because PerfectMail strongly favors users and peers with an established reputation, it is safe to reduce **Tag** and **Reject** thresholds without the risk of introducing false-positive scores.

Optimal settings need to be determined empirically because each PerfectMail interacts with a unique set of users, mail peers and mail servers. To assist you with setting up your new appliance, we suggest the following settings based on our own experience with the product:

	Tag	**Reject**
Initial Deployment or for each new Domain	16	26
Retail ISP and non-business settings	14	24
Safe long term settings	12	22
More aggressive long term settings	11	18

Unfortunately, some spam will score under 26 and may score under 16 so your users will still encounter unwanted messages. However, PerfectMail is highly effective right "out of the box" so the amount of unwanted messages should be dramatically reduced.

11.2.3 Uncertain Message Disposition (Tagged Messages)

PerfectMail™ prepends a *tag phrase* (`[SPAM?]` by default) to the subject line of any Tagged messages. PerfectMail records the details of each message in its reputation system so that, as the sender's reputation is established, PerfectMail will be less likely to **Tag** that senders messages.

Concerns can occasionally arise in your user community when a low frequency (or first-time) legitimate sender has receives a Tag score (and the `[SPAM?]` marker) on the subject line.

After a week administrators should take time to fine-tune PerfectMail so that the number of Tagged messages is safely and accurately reduced. A few moments spent fine-tuning PerfectMail will result in a more pleasant experience for users (fewer Tags) and fewer support calls for administrators.

11.2.4 Why Tag Messages?

We know that correctly handling legitimate e-mail is much more important than blocking spam. We designed PerfectMail™ to quickly and accurately discriminate between unwanted e-mail from unknown senders and valuable e-mail from your established *e-mail peers*.

PerfectMail accomplishes this task through adaptive learning. PerfectMail watches all e-mail traffic and quickly learns who e-mails whom. Once e-mail relationships are established, PerfectMail auto white lists the e-mail peer.

PerfectMail can discover e-mail peer relationships between active e-mail peers in as little as a few hours to a few days; and this happens automatically.

11.3 Real-Time Block Lists

Real-time Block Lists (RBL) are databases of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services). These lists are the result of the combined multinational effort to eradicate spam.

PerfectMail™ subscribes to several high quality RBL services along with its own proprietary services.

If your e-mail peers are being rejected due to RBL sites, then there has been some issue with their servers. To stop the messages being blocked, they either need to fix the problem and get de-listed; or you can add their domain to the *No Host Checks* table in the user interface.

11.4 Anti-Virus

Anti-Virus software examines your e-mail for known rogue software, including computer viruses, worms and dangerous files. Additionally our anti-virus engine has been leveraged to identify known phishing scams and social engineering scams. All such content has the potential to harm your users and your company.

Additionally, PerfectMail™ lets you filter out e-mail attachments which may be dangerous to your users.

PerfectMail offers professional grade anti-virus filtering with ClamAV. To stay up-to-date, your PerfectMail product checks for virus signature updates automatically every ten minutes.

Important: PerfectMail anti-virus filtering cannot replace your *desktop anti-virus software*. Sometimes e-mail can contain *web links* to viruses and executable files that PerfectMail simply can't block. We check all *web links* against a list of known malware sites, but this kind of filtering is far from perfect. You still need to rely on your *desktop anti-virus software* to analyze and block viruses and malware at the desktop.

11.5 *Grey-Listing*

Grey-listing is a technique where incoming e-mail messages are temporarily delayed before being accepted. This can be an effective technique in blocking spam. Here's how *grey-listing* works in PerfectMail™.

Grey-listing forces a delay in the message delivery. It forces the sending server to try to resend the message at a later time, usually within 10 to 30 minutes. The *grey-listing* scheme makes use of normal e-mail server behavior. This sort of thing happens quite often with mail servers.

PerfectMail performs its normal analysis of the e-mail. If the score of the message is higher than your tag threshold and the sender has never before sent you a good message, this message is temporarily delayed. This is not a "real" failure. The server says, "I can't receive that message right now, try again later." Most spam engines will not come back, while all legitimate mail servers will. After 3 minutes or 3 attempts to send the message (whichever comes first) the message will be accepted.

PerfectMail has a module that maintains an ongoing list of all machines that have been *grey-listed*. It double checks to ensure the message will come through without too much delay.

Grey-listing may also be used on messages that appear to be newsletters or spamvertizing. These two types of e-mail are extremely similar and hard to distinguish. If the score is high enough or if specific triggers are found in the message these types of e-mail will be *grey-listed*. Newsletters are not usually time sensitive. Still, after a few messages are exchanged, *grey-listing* will no longer occur for the sender.

If delaying messages becomes an issue, you can turn off *grey-listing* on the *Web Based User Interface (Web-UI) Filter Setup* page.

11.6 Spam Traps

Spammers are constantly scouring the Internet looking for fresh targets for their trash. Empirical studies show that Spammers harvest e-mail address from web-sites, discussion groups, web blogs, chain letters and any other source they can find.

Spammers are so effective at harvesting e-mail addresses from websites that some people report receiving spam on their website published e-mail address in as little as 8 hours from the time the e-mail address is first posted to the site. It is because of aggressive website e-mail harvesting that many people believe that it is no longer practical to publish your e-mail address on your company or personal website.

PerfectMail™ is so effective, you can safely publish your e-mail address on your web site.

Surprisingly, an effective way to defend against spam is to give Spammers exactly what they want! PerfectMail includes a feature aptly called *Spam Traps*. Spam Trap accounts are e-mail addresses that are used to trick Spammers into identifying themselves.

The Spam Trap strategy is simple; create a bogus e-mail account, hide that account on your website, let Spammers harvest the bogus address from your website and then block all e-mail traffic that includes the Spam Trap e-mail addresses in a message's recipient list.

PerfectMail's *spam trap* feature looks for pre-defined Spam Trap e-mail addresses in the recipient list of every in-bound message. If a Spam Trap e-mail address is found in the recipient list, PerfectMail will:

1. Quietly removes all legitimate e-mail addresses from the recipient list (so legitimate users don't receive spam).
2. Adds or updates its reputation system to mark the sender as a Spam Trap spammer.
3. All the *real recipient* e-mail addresses are rejected to encourage them to "prune" your valid e-mail addresses from their lists.
4. All the *spam trap* e-mail addresses are accepted to encourage the spammers to keep using them.
5. Silently discards the message.

This strategy is effective because it gives PerfectMail notice when a spammer is targeting your server.

11.6.1 Filters > Spam Traps

Spam Traps are *fake e-mail addresses* that are used to catch spammers.

Spammers use harvesting engines to walk websites gathering e-mail addresses. Add *spam traps* to your website to *poison* the spammer's address lists. Publish *spam traps* on your website in non-obvious ways; like white on white text, or using an extremely small font.

When the spammer tries to e-mail the *spam trap* PerfectMail™ knows who they are and will block any further activity.

List one e-mail address per line.

Example:

```
honeypot@mydomain.com
```

11.7 Rejecting Spam

On any type of *reject*, a message delivery failure is *immediately* returned to the sending mail server. This occurs during the actual e-mail transaction which ensures a guaranteed delivery to the sending server.

Because PerfectMail™ never *accepted* the e-mail, the *responsibility* for dealing with that e-mail lies with the sending server. This behavior is markedly different from many *delivery failure* messages which are generated after a message has been accepted, scanned, then deemed to be spam.

This is a subtle difference but an important one. This ensures the *responsibility* for the e-mail lies with the sending server. We avoid the potential responsibility for such messages and avoid any legal requirements for storage, archiving, etc. that may otherwise be implied.

Further, many *delivery failure* messages are sent to spammers who do not accept them. This can literally choke your e-mail infrastructure with garbage messages that will never be sent.

11.8 False Positives

False Positive
    Legitimate e-mail that is falsely rejected by an anti-spam product.
False Negative
    Spam e-mail that is falsely accepted by an anti-spam product.

No e-mail scanning solution can be 100% effective. There is always a trade off between accepting spam and rejected legitimate e-mails. **Our Goal: Zero false positives**

The key to achieving zero false positives is in PerfectMail's history and reputation engine. By watching and recording e-mail activity, PerfectMail learns the identity of your *e-mail addresses* and their *e-mail peers*; as well as building and learning the reputations of both known and unknown mail servers.

PerfectMail learns and remembers who you e-mail, so we can let those messages through.

11.8.1 A Note on Anti-Obfuscation and Suffix Matching

Anti-Obfuscation is a series of techniques used to identify attempts to side-step spam filters by making minor modifications to words and phrases. Often punctuation, repeated letters, substituted similar looking characters and insertion of whitespace is used to attempt to hide words and phrases from spam filters.

Suffix Matching is a technique used to extend a word using a variety of word suffixs. For example, if you wanted to score the word *jump* the *Variable Suffix* engine could also catch: *jumps*, *jumping*, *jumped*, *jumpy*, *jumper*, etc.

It's very important to understand the impact of **anti-obfuscation** and **suffix matching** when matching phrases in the content filters. These techniques try and match your words and phrases by matching possible *variations* that may be used to try and avoid detection.

This becomes a problem when you are trying to match a *specific phrase*. For example, if you try and match the word *"reporrrt"* when looking for spam and have *anti-obfuscation* turned on it will also match *"report"*, which will likely cause a lot of false postives.

This becomes even more problematic when both *anti-obfuscation and suffix matching are both enabled. So using our example "reporrrt", you would also match "report", "reports", "reporting", "reported", "reporter", etc.*

These are powerful tools, but need to be used with some forethought and caution.

11.9 E-mail Recovery

Rather than having a *quarantine*, PerfectMail™ has a short term message storage facility where it keeps a copy of **all e-mail** that has passed through it, including a copy of most of the e-mail that PerfectMail *rejected*.

Not only can you release messages that may have been inadvertently rejected, but you can also resend messages that may have been lost for some other reason.

In fact, if you lose your *whole mail server* you can recover your e-mail by using the *Message Replay Wizard* to simply re-transmit any lost e-mail activity.

If your mail server does stop functioning, PerfectMail will identify and spool up your e-mail and automatically forward it to your mail server when it comes back up. Then, if necessary, you just replay the lost time period. Easy!

11.10 Filter Settings

11.10.1 Filters > Filter Settings

Filer Settings: General

Demo Mode - In demo mode your PerfectMail™ server will perform *no actual e-mail filtering*. The user interface will report the decisions PerfectMail *would have taken*, but *no actual filtering will take place*.

Grey Listing - Grey Listing is a technique where e-mail servers are *temporarily rejected* the first few times they try to send e-mail. Legitimate e-mail servers will always resend the message. A great deal of *spam* comes from compromised PC's and industrial spammers, which will likely not resend messages. Grey listing may also occur in specific circumstances that highly indicate spam. When grey-listing occurs, senders receive a temporary reject until one of the following occurs:

- **3** minutes has passed
- more than **3** messages have been sent
- a message scores more than the *tag threshold*
- or, *Grey Listing* is turned off

Grey list data miners - A mail server is considered to be a "data miner" when it regularly attempts to send e-mail to non-existant e-mail addresses within your domain.

Delay new address queries - Upon initial installation, all of the e-mail addresses in your domain(s) are new to PerfectMail™. This option should be left off during the first month of operation so that the software can learn who are the valid recipients within each domain your are administering. After the first month, you can turn this option on to help deflect data miners. New employees should be asked to send an initial e-mail to an external address so that the system can recognise a valid, new e-mail address.

Strict check vulnerable domains - For certain domains which are primary targets of phishing e-mails, PerfectMail™ performs an extra set of validation checks.

Block Missing PTR - Best e-mail practices include ensuring your e-mail server has a *reverse DNS record* (PTR record). Many compromised computers do not have this, so it is a good way of identifying spam sources. Unfortunately, there are quite a number of mail servers that don't follow *best practices* so there is a potential for false positives. Use with caution.

Reserved Percentage - Let's say your license allows you to have 100 simultaneous e-mail connections and you have reserved 10% for e-mail servers you have exchanged e-mail with before (they are "known"). If your server is handling 80 simultaneous connections with known e-mail servers, 10 will be left available for new e-mail messages from known e-mail servers, and the remaining 10 will be used for handling e-mail traffic from unknown e-mail servers.

Filter Settings: Attachments

- **Block Attachments** - Any attachment with executable commands can possibly damage/infect the recipients computer. Block e-mails containing dangerous e-mail attachments.
- **Zipped Attachments** - Block zip files containing dangerous file types.
- **Attachment List** - A scrollable list of the file types you wish to block. New file types can be added to the list, one file type per line.
- **Score links to dangerous attachments** - Increase the spam score of an e-mail if a link to a dangerous file type is present.
- **Dangerous link score** - The amount to add to the total spam score of the e-mail when a link to a dangerous file type is present.
- **Attachment List** - A scrollable list of the file types you wish to block links to. New file types can be added to the list, one file type per line.

Filter Settings: Reputation

Sender Policy Framework (SPF)

Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery. It allows the owner of a domain to specify their mail sending policy (which mail servers they use to send mail from their domain). If a message comes from an unknown server, it can be considered a fake and rejected. Since policies like *SPF* are relatively new, organizations may incorrectly structure their *SPF* records, blocking their own mail from being delivered to remote sites. If this is an issue for your organization, you can disable *SPF Filtering*. For more information on *Sender Policy Framework* please visit http://www.openspf.org.

- **Enable SPF Scoring**: If you are experiencing major problems with SPF filtering you can disable it here. If you have problems with specific domains try adding them to the **No Server Checks** table on the **Incoming Sender Settings** page.
- **SPF soft fail score**: The administrator for the senders domain says the sender is **probably** not from their organization. Score this amount.
- **SPF hard fail score**: The administrator for the senders domain says the sender is **definitely** not from their organization. Score this amount.
- **Peer status over-rides RBL/SBL** - At some point a mail server that you have a long history of exchanging e-mail with will become black listed. Enabling this option results in the history overriding the sudden appearance on a black list. This will allow e-mail to continue to flow from the listed server. All e-mail content will still be analyzed to see if it is spam.

RBL Lists - Real-time Block Lists. *These options should always be turned on.* Real-time database of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services). We use the following services:

- **SWL List** - Enable the Spamhaus White List. This is an active, validated list of known good e-mail servers. Mail server IP addresses listed here are given a bonus score.
- **RBL** - Miscellaneous RBL Lists: Various RBL lists that are not yet classified into categories in the PerfectMail interface.
- **SBL** - Spamhaus Block List: This table is maintained by a dedicated international team based in eight countries, working 24 hours a day, 7 days a week.
- **PBL** - Policy Block List: A list of end-user IP address ranges which should not be delivering unauthenticated e-mail to any Internet mail server.
- **XBL** - Exploits Block List: A real-time database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, Wingate, etc), worms/viruses with built-in spam engines, and other types of Trojan-horse exploits.
- **CBL** - Composite Block List: The CBL takes its source data from very large spam traps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, Wingate etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of Trojan-horse or "stealth" spam ware, without doing open proxy tests of any kind. (cbl.abuseat.org)
- **CSS** - Snowshoe spammers frequently use many fictitious business names (DBAs), false names and identities, concealed anonymous domains and frequently changing postal dropboxes and voicemail drops to prevent others from connecting snowshoe spam operations to one another and recognizing who is behind the operations and the spam they send.
- **NJABL** - Open Proxy IPs List: This service performs automated open relay and open proxy tests against any system that connects to any of the SMTP servers on networks that contribute relay data to the list. (www.njabl.org)

Additional RBL Service

PerfectMail automatically makes use of a number of RBL services, including the Spamhaus RBL services. You can add an additional service here:

- **RBL Host** - The host name used for performing RBL look-ups. The RBL look-up will be performed using current conventions. For example, looking up address 1.2.3.4 on the RBL host *lookup.myrbl.com* will generate a DNS look-up of *4.3.2.1.lookup.myrbl.com*. If PerfectMail receives a response of *127.0.0.?* (where ? is any value), the message will be deemed RBL listed.
- **RBL Reject Message** - This text will be returned to the message sender. It's a good idea to direct the sender to a website that will describe why their message was rejected. To make this possible you can use the **{ADDR}** macro to insert the sender's IP Address in your message.

Filter Settings: Spoofing

Domain Spoofing Filter

Often spammers will send messages that reportedly come from a domain you host. This section allows you to filter e-mail originating from the outside, which contains one of your domain names in the *from* e-mail address. Options are to:

- **Verify e-mail address.** Verify the existence of the sender address. The sender address must exist on the local server.
- **Block self sent e-mail.** That is, e-mail originating from the outside world, where the from and to address are the same, will be blocked.
- **Block all.** All e-mail that reportedly comes from one of your hosted domains, but originates from the outside world, will be rejected.

Filter Settings: Content

E-mail content is compared against the list of scored words in both the subject and body word lists as well as the Bayesian filter.

Use system word list - Use the word list provided by PerfectMail™. You can view the word list at "Filters > Content > System Word List".

Use local word list - Use the word list that you can edit. You can edit/view this word list at "Filters > Content > Local Word List".

Maximum word score - subject - This is the maximum amount that will be added to the total spam score of the message based on the content of the subject line. So if the spam score of the subject line exceeds the maximum, only the maximum value will be added to the total spam score of the e-mail. Words and phrases that have a spam score of 99 in the system and local word lists are not affected by this limit. The value 99 is special, it indicates automatic rejection. Default value for this field is 16.

Maximum word score - body - This is the same as maximum word score - subject except it applies to the actual message body. Default value for this field is 16.

Bayesian filter - Enable the Bayesian filter subsystem. Bayesian filtering is a technique that uses statistical analysis to calculate the probability of an e-mail being spam; based on past history. PerfectMail constantly examines messages and self trains to ensure the Bayesian database is updated as spam changes.

Maximum Bayesian score - Default value for this field is 16.

Maximum Bayesian bonus - This is the maximum value that the total spam score of the message can be REDUCED if it's Bayesian score indicates that it is a good e-mail. Default value for this field is 3.

Content profiling - Enable the spam profiling subsystem. Default, checked.

Maximum profiling score - Default value for this field is 16.

Spamvertizers are industrial spammers who send seemingly legitimate advertising. They send large volumes of spam from ever changing server IP's, domain names and company names.

Enable Spamvertizer analysis - Default, checked.

Maximum Spamvertizer score - This maximum works in the same way as Maximum word score - subject. The value you enter should result in messages being rejected. Default value for this field is 16.

Phishing is the act of spoofing a legitimate site to try and gain personal information such as userid's, passwords, banking information, etc. Financial institutions are often the targets of phishing attacks.

Phishing Analysis - Default, checked.

Phishing score - This score should reject messages. Default value for this field is 16.

Filter Settings: Websites

PerfectMail extracts web site addresses (URLs) from e-mail messages and checks them against known spam sources and compromised servers and networks. As part of e-mail analysis, some websites may be examined to determine what sort of content they host. During the analysis process portions of the website may be downloaded to PerfectMail and cached.

Be aware that some web probes may contain hashed or encoded versions of your users e-mail addresses. We take reasonable steps to avoid any links that may include e-mail addresses or cause specific user based behavior (e.g. subscribe, unsubscribe). However, due to URL obfuscation methods we can not be completely accurate in eliminating all such links.

URLs extracted from the website, including website redirects are checked against various known spam site databases and scored against various lists to the specified maximum website URL score:

- **RBL** - Domains listed on the RBL lists.
- **DBL** - Domains listed on the domain block list.
- **SURBL** - Domains listed on the SURBL list.

Enable website probing - Results in the structure of the referenced website being tested for suspicious behaviour. For instance, if the URL points to a website which redirects you to a second website which redirects you a third website, etc. This would be an instance where we would consider the URL to have a malicious / spammy intent.

Website content analysis - The contents of the website are analyzed with the same tests used to determine if an e-mail is spam.

Maximum web score - It should be noted that this maximum score represents the sum of the *Maximum website URL score* plus any additional spam points from *Enable website probing* and *Website content analysis*.

URL history size - The number of website URLs to be kept in history.

Google Safe Browsing - Uses Google's list of suspected Phishing and Malware pages.

Filter Settings: Outbound

This feature allows you to filter your organization's outgoing e-mail.

Filter outbound recipients - uses the Black and White lists on **Filters > Sender** to block recipients for outbound e-mail. The black list will normally prevent a specific domain or address from sending to your server; this switch allows you to block traffic destined for those senders as well.

Filter outbound senders - restricts which domain names a *sender* may use for *outgoing* e-mail. Restricting outgoing e-mails can help prevent infected computers inside your network from sending spam, viruses and worms to the Internet. You can specify three types of filtering:

- **No filtering**
- **Allow sub domains of configured domains** - E-mail may be sent by configured domains and their sub domains. For example, if *mydomain.com* is configured in PerfectMail then outgoing e-mail such as *myname@myhost.mydomain.com* will be allowed.
- **Allow only configured domains** - Only allow e-mail from configured domains. All outgoing e-mail *must* be from a configured domain.

Other outbound sender domains - You can use this list to specify other, non-PerfectMail configured, domains to be e-mail senders.

Content filtering - applies the subject and body content reject filters to your outgoing e-mail. You can specify three types of filtering:

- **No filtering**
- **Partial content filtering** - blocks e-mail if it contains words and/or phrases that score 99 in the *reject words* list.
- **Full content filtering** - analyzes the outgoing message in its entirety. If it scores above the *Reject Threshold*, then the e-mail is blocked.

Exempt recipients - Used to specify recipients that do not require e-mail filtering. Enter domain names / IP addresses into this list, one per line. (Example: Use this for forwarding e-mail to blackberry.net.)

Filter Settings: Actions

If PerfectMail is uncertain about an e-mail, the subject line is *tagged* with the text defined here. The default setting is **[Spam?]**. Administrators should monitor their *tagged* messages. If the number of legitimate messages being tagged is high, the spam thresholds may need to be adjusted. *Our goal is to reduce the number of tag messages received to zero.*

- **Tag messages** - Enable subject tagging of uncertain e-mails.
- **Spam tag** - Define the spam tag. Default: [Spam?]
- **Remove outgoing tags** - Remove tag messages from outgoing e-mails, specifically replies to tagged messages.

Rejecting Spam

By default, PerfectMail will reject any message found to be spam. It returns a failure code, the reason for the failure and the text contained in the *reject message*. You can also choose to not *reject spam*; instead making use of the *mail headers* to filter e-mail at the mail client. (However, we recommend filtering e-mail at the server.)

In most instances the text in the **Reject Message** edit box will be forwarded to the person who sent the rejected e-mail. If a message is falsely rejected, this is the message the sender will see. It's a good idea to describe a method of contacting your e-mail support staff.

Mail Headers

All e-mail messages have headers which are typically not shown by your e-mail client program. E_mail headers include the From:, CC:, and Subject: fields you normally see when processing your e-mail. The message headers section of an e-mail contains extra information, such as the actual sender of the message which, when dealing with spam, is almost always different than the name stated in your From: field.

PerfectMail can be configured to add spam info headers to your e-mail messages. Your can use these headers to filter e-mail right at your e-mail client (e.g. Microsoft Outlook).

- **Spam score header** - This creates the *X-PM-Score* message header. This message header displays the numeric *spam score* of the message. Example: X-PM-Score: 15
- **Spam flag header** - This creates the *X-Spam-Flag* message header. This message header displays *YES (or NO)* if the message is spam (or not). Example: X-Spam-Flag: YES
- **Spam level header** - This creates the *X-Spam-Level* message header. This message header displays a graphic representation of the *level of spaminess* using *'s (each * represents 4 points of *spam score*). Example: X-PM-Score: ****
- **Outgoing mail headers** - Suppress adding the above e-mail headers to outgoing messages.

Strip outbound DKIM - Strip inbound DKIM - At this point in time, PerfectMail™ does not make use of DKIM headers.

11.10.2 Filters > Sender

Formerly Black/White List

The following tables adjust filtering for mailhosts, domains and e-mail addresses. Using these tables it is possible to block content for whole countries. The following tables are availabe:

- **White List** - Mail servers, sending domains and e-mail addresses listed here will not be blocked by the spam filter, unless the e-mail contains a virus. List known good servers here to ensure important e-mail does not get blocked. Web servers and other production servers may send e-mail notifications, but these servers are often poorly configured as mail servers, making them good candidates for white listing.
- **Black List** - Mail originating from servers and domains listed here will be rejected.
- **Discard List** - Mail originating from servers and domains listed here will be quietly discarded. Note: this does not affect filtering or scoring decisions, which will occur as is normal. However, regardless of the result of the filtering system, the message will be quietly discarded.
- **No Reject List** - Similar to the *Discard List*, this table lists servers and domains what should not receive reject messages. This is especially important for newsgroup services such as *Yahoo Groups* which may react negatively to anti-spam software. For example, if messages forwarded from *Yahoo Groups* are rejected, *Yahoo Groups* may stop forwarding messages to the protected e-mail address. Listing such servers here allows you to quietly discard spam without affecting the delivery of future messages.
- **No Server Checks List** - Servers listed here, either explicitly by hostname or IP address, or implicitly as members of some domain, will not receive any server based validation or reputation checks, including SPF and RBL lookups. Servers that become black listed by RBL lists or have SPF configuration problems are good candidates for adding to this list, allowing you to accept e-mail from such servers and domains regardless of their disposition on such lists.

Table Format:
Each table accepts entries using the following formats. Certain format types may not make sense for all tables; please refer to the appropriate table description below for more information. The following formats are supported:

- **IP Address:** *X.X.X.X* or *X.X.X.X/Y* - to specify an IP address or net block. For example:

```
192.168.1.3
192.168.2.0/24
```

- **Host Name:** Specify the Fully Qualified Domain Name (FQDN) of a specific host. All hosts and subdomains contained within a specified domain will be included in the match. (e.g. listing 'porn' would block all domains ending in '.porn'.) There should be no leading dot. Two wildcards are supported for domain name matching, '*' for matching multiple characters and '?' for matching a single character. For example:

  ```
  myhost.domain.com
  yourhost.yourdomain.com
  spamdomain.*
  porn
  ```

- **Domain:** Specify a complete domain, including sub domains. All hosts and subdomains contained within a specified domain will be included in the match. Each portion of the domain name must be specified fully unless wildcards are used. There should be no leading dot. Two wildcards are supported for domain name matching, '*' for matching multiple characters and '?' for matching a single character. For example:

  ```
  newyork.customer.com
  company.com
  ```

- **E-mail Address:** Specify complete e-mail addresses. This is particularly useful for domains that commonly send spam. There should be no leading dot. Two wildcards are supported for domain name matching, '*' for matching multiple characters and '?' for matching a single character. For example:

  ```
  user@domain.com
  ```

- **User:** Specify the user portion of an e-mail address. This is useful for specifying commonly used e-mail addresses, across multiple domains. For example:

  ```
  sales@
  webmaster@
  ```

11.10.3 Filtering > Subject

Subject Filter

The subject line of each message is checked for the listed words and phrases. The word list is case-insensitive and treats all punctuation as spacing. Your words will be automatically converted to the simplest version our filter can handle, including character case conversion and stripping of punctuation. Our anti-obfuscation engine is quite effective but should be used with caution.

Subject word categories:

- **Reject words** - Words and phrases contained on this list (one per line) cause the e-mail to be rejected.
- **Scored words** - Words and phrases contained on this list are given a score as specified in the *score field* just below the word list boxes.
- **System words** - These words and phrases are maintained by PerfectMail™.

Anti-obfuscation is a technique that identifies attempts to disguise words. For example:
Anti-Obfuscation maps `\/ 1 @ g r @` to `viagra`, `><@n@x` to `Xanax`, etc. The word score is scaled to match the measure of obfuscation. This technique is very successful, but it can sometimes give erroneous results if the listed word is similar to other non-offensive words; use with care. In particular try to avoid very simple words that may appear in messages; for example a word such as "aaaa" would be a very bad word choice.

Note: Only use alpha characters in the words and phrases. Do not use punctuation or special characters because the anti-obfuscation engine skip past these characters. Similarly, avoid accented characters.

To avoid false rejects, take special care when selecting words for these lists.

11.10.4 Filtering > Body

Body Filter

Use this filter to identify messages containing content and language that is not acceptable to your organization. When adding entries to this table, please take some time to consider the various instances where these phrases may be used; and may trigger false positives.

The body of each message is checked for the listed words and phrases. PerfectMail™ uses a custom content analyzer that utilizes a restricted alphabet to efficiently parse out words. All phrases are case-insensitive and all punctuation are treated as spaces.

Your words will be automatically converted to the simplest version our filter can handle, including character case conversion and stripping of punctuation. Our anti-obfuscation engine is quite effective but should be used with caution.

Body word categories:

- **Reject words** - Words and phrases contained on this list (one per line) cause the e-mail to be rejected.
- **Scored words** - Words and phrases contained on this list are given a score as specified in the *score field* just below the word list boxes.
- **System words** - These words and phrases are maintained by PerfectMail™.

Anti-obfuscation is a technique that identifies attempts to disguise words. For example:
Anti-Obfuscation maps `\/ 1 @ g r @` to `viagra`, `><@n@x` to `xanax`, etc. The word score is scaled to match the measure of obfuscation. This technique is very successful, but it can sometimes give erroneous results if the listed word is similar to other non-offensive words; use with care. In particular try to avoid very simple words that may appear in messages; for example a word such as "aaaa" would be a very bad word choice.

Note: Only use alpha characters in the words and phrases. Do not use punctuation or special characters because the anti-obfuscation engine skip past these characters. Similarly, avoid accented characters.

To avoid false rejects, take special care when selecting words for these lists.

11.10.5 Filters > Vacation

Vacation Message Exclude Filter

PerfectMail™ uses e-mail traffic history to build a database of who your e-mail peers are. Vacation messages or "Out of Office" messages can skew these results as they indiscriminately send responses to everyone, including spammers.

To avoid rewarding spammers for receiving such messages, the subject and body (if selected) of outgoing e-mails are scanned for the phrases listed in this table. E-mails that match are delivered normally, but they are not used for database training purposes. This ensures vacation message responses sent to spammers will not give spammers a favorable history.

List vacation phrases in the following table, one entry per line. Subject lines are scanned automatically. Optionally, you can select to also scan the message body.

For example:

```
Vacation message
Out of the office
```

12 E-mail and Web Content Disclosure

PerfectMail™ accesses, examines, analyzes, downloads, logs and filters e-mail content. **Such content may may be offensive or illegal.** (Which is why we're trying to stop it.) You should be aware that such e-mail content exists and may be logged and retreived in the *User Interface*.

As part of e-mail analysis, some websites may be examined to determine what sort of content they host. During the analysis process portions of the website may be downloaded to PerfectMail and cached.

Be aware that some web probes may contain hashed or encoded versions of your users e-mail addresses. We take reasonable steps to avoid any links that may include e-mail addresses or cause specific user based behavior (e.g. subscribe, unsubscribe). However, due to URL obfuscation methods we can not be completely accurate in eliminating all such links.

Be aware that web probes originating from your PerfectMail server are automated probes, not user based actions. This is especially important if your PerfectMail server accesses websites through a "web proxy". In that situation it is your responsibility to differentiate between PerfectMail accessing websites and similar actions by your users.

If necessary, you can disable **Web Content Filtering** via the Web Interface: **Filtering => Filter Settings**

13 Managing E-mail

13.1 Protected E-mail Addresses

PerfectMail classifies e-mail into two categories: Inside *Protected Addresses* and *Outside Addresses*. *Protected Addresses* are those e-mail addresses used by your organization and protected by PerfectMail. All other e-mail addresses are in the *Outside* category and not tracked or indexed.

This is an important distinction that impacts how you search for e-mail. PerfectMail only "knows" it's *Protected Addresses*.

13.1.1 Domain Admin > E-mail Addresses

Use these tables to explicitly configure e-mail addresses for all domains. It's important to ensure PerfectMail™ can identify which e-mail addresses are valid on your servers, so it can avoid loading your servers with unnecessary e-mail traffic and avoid overloading your mail server with *Delivery Status Notification* messages for bogus senders.

PerfectMail uses two methods of e-mail address validation, which work together to identify e-mail address hosted by your server:

1. **SMTP Validation** - A validation technique that directly queries your mail server via SMTP queries. For this option to work you must ensure that *SMTP Recipient Filtering* is enabled in your mail server; otherwise PerfectMail may become swamped with bogus information. If this is the case, turn off *SMTP Validation*. If *SMTP Validation* is turned off PerfectMail will build it's own table of addresses by watching your outgoing e-mail. *SMTP Validation* can be enabled via the *Domain Admin* page.
2. The **E-mail Addresses** tables - to explicitly define e-mail addresses. These tables can work in conjunction with *SMTP Validation* or on their own. The available tables are described below.

Table Format:
For each table, list one e-mail address per line. For example:

```
user@mydomain.com
user@myotherdomain.com
```

"Valid" Addresses:
Use this table to create a global list of **valid** e-mail addresses hosted by this PerfectMail server. Use this table in combination with your *SMTP Validation* as a set for each domain.

"No Filter" Addresses:
Use this table to explicitly list e-mail addresses that are valid, but should receive **no anti-spam filtering**.

"No Filter Attachment" Addresses:
Use this table to explicitly list e-mail addresses that are valid, but should receive **no attachment filtering**. Most users do not need to receive potentially dangerous e-mail attachments (e.g. executable code), but some users need such files as part of their regular communications. You can turn on dangerous attachment filtering for your user population, but still allow specific e-mail addresses to receive potentially dangerous files.

"No Deliver" Addresses:
Use this table to explicitly list valid e-mail addresses that we *should not* accept messages for. Sometimes internal e-mail addresses, including distribution lists, are identified by spammers. This table helps to keep your private address

private.

"No Store" Addresses:
Use this table to explicitly list valid e-mail addresses that we should not store **message content** for. Use this table to avoid storing e-mail for particularly security conscious users.

13.2 Discovered Users

PerfectMail has auto-discover functionality to learn your organizations e-mail addresses. This reduces the work load on the mail admin in having to maintain user lists in multiple places.

PerfectMail uses *discovered users* to record e-mail traffic statistics to build relationships between e-mail peers, to aid with anti-spam decisions.

The PerfectMail server builds up a list of users by watching e-mail traffic. PerfectMail can be configured to query your mail server using *SMTP Recipient Filtering* for e-mail address validation. To reduce the volume of new address requests from data miners a filter may delay first time sender/recipient combinations. (You can turn this off in "Filtering >Filter Settings" by disabling *Delay new address queries* under *General Filter Options*.)

Addresses are removed from the list of Discovered Users, when the e-mail activity for an address drops to zero over an extended period of time and your mail server no longer reports the address as being valid.

13.3 Tracking E-mail with Message IDs

Each e-mail message is assigned a unique *Message ID* (e.g. o7IBY66I013204) by each mail server the message is relayed through. Often these *Message ID's* are recorded by the mail server in a *Received:* e-mail header. The PerfectMail message view page shows the *Message ID* for each message at the top of the page.

You can use the *Message ID* to locate e-mail exchange details in the *Transmission Log* for a specific message; or inversely use the *Message ID* from the *Transmission Log* to locate and display the contents of an actual e-mail.

When tracking the progress of an e-mail, take a close look at the "stat=" portion of log entries in the Transmission Log. The "stat=" will say what happened to the e-mail and will often give the *Message ID* that was assigned to the message on the mail server it was sent to.

13.4 Searching for E-mail

The PerfectMail™ *Web-UI* has some useful features under that *Activity* menu for searching for specific e-mail addresses. There are two types of reports under this menu: a *Transmission Log* and a selection of *Mail Log* views.

The *Transmission Log* page displays e-mail activity from the point of view of the *Mail Transport Agent* (MTA). The data shown has to do with e-mail transactions as opposed to e-mail content. This log is very useful for investigating problems with e-mail delivery. All e-mail activity is recorded here; including e-mail delivery attempts that failed or were incomplete.

All the other views under this menu are concerned with actual e-mail messages. All successful e-mail transactions are shown here, whether the messages were accepted or rejected. You can search for and view messages and how they were filtered.

If you want to find a message and how it was filtered use one of the *Mail Log* views. If you want to see if the remote mail server was able to communicate with PerfectMail at all use the *Transmission Log*.

The *Transmission Log* is also useful for finding out why an outgoing e-mail may have been rejected by a remote mail server. The response from the remote mail server should be included in the *stat=* field of the SMTP transaction.

The E-mail Address search fields can **only** search for *protected e-mail addresses*. This applies to all e-mail address search fields.

When searching for a specific e-mail, search for the *Protected Address* of your organization to narrow the search down. You can further filter the search by putting the *Outside Address* in the *Search* field.

(Searching in the *Transmission Log* view is purely a text based search.)

13.4.1 Date Field Format

Notes on date field formatting for all PerfectMail™ user interface pages.

Many of our web pages reference date/time ranges. There are many date/time syntax's available. To remove ambiguity, PerfectMail standardizes on the following date/time format using 24-hour clock values:

```
YYYY-MM-DD HH:MM
```

Where YYYY-MM-DD is a 4-digit year, 2-digit month (e.g. 04 for April) and 2-digit day; and HH:MM is a 2-digit hour and 2-digit minute.

The complete *syntax* is

```
[[[YYYY-]MM-]DD ]HH[:MM]
```

which allows for the following variations:

```
YYYY-MM-DD HH:MM
YYYY-MM-DD
YY-MM-DD HH:MM
YY-MM-DD
MM-DD HH:MM
MM-DD
DD HH:MM
HH:MM
HH
```

Blank date/time values are assumed to extend the date range *forever* in the past or present as appropriate; unless doing so would result in an unreasonable amount of data, in which case a reasonable date value will be substituted.

All date/time values are assumed to be in your *PerfectMail™* server's local timezone.

13.4.2 Activity > Mail Queue

The *mail queue* page shows messages queued for delivery, both incoming and outgoing. Message queuing is a normal activity; in fact all messages are queued if only for a short time. It is normal to have a number of messages in the *mail queue* waiting for transmission.

E-mail deferral occurs when a message (usually outgoing) can not be immediately handed off to the next relay host. It is quite common to have messages queued as "deferred" as remote mail servers may not be available for any number of reasons: network traffic congestion, service outages, server load, DNS hiccups, grey-listing, etc.

Sometimes *spam* and *delivery notification messages* will get stuck in the queue as well. Spammers send a lot of e-mail, but rarely accept return e-mail, including bounce messages. These messages can get stuck in the queue. PerfectMail™ has automated processes that clean out such messages on an hourly basis.

Some interesting information on queue processing:

- Message delivery is retried every 15 minutes.
- Messages are resent in *priority order*. (You can set the *message priority* using your e-mail client.)
- A *warning* will be sent to the sender for queued messages after the following times:
    - ♦ **Urgent** priority messages: 1 hour
    - ♦ **Normal** priority messages: 4 hours
    - ♦ **Non-urgent** priority messages: 12 hours
- For failed delivery, the message will be *bounced* back to the sender after the following times:
    - ♦ **Urgent** priority messages: 1 days
    - ♦ **Normal** priority messages: 3 days
    - ♦ **Non-urgent** priority messages: 5 days

If message viewing is permitted, clicking on the subject line will display the e-mail contents and the reason for its delay (highlighted in yellow).

You can use the **Delete Selected Messages** link to immediately remove unwanted messages from the queue. Simply mark the check box beside each message to be deleted, or click *toggle all*, and click the *delete selected messages* link.

Messages are automatically resent every 15 minutes.

13.4.3 E-mail > Transmission Log

Transmission Log Viewer

The *Transmission Log* page displays e-mail activity from the point of view of the *Mail Transport Agent* (MTA). The data shown has to do with e-mail transactions as opposed to e-mail content.

This log is very useful for investigating problems with e-mail delivery. All e-mail activity is recorded here; including e-mail delivery attempts that failed or were incomplete. For example, if you are investigating an issue where you expect e-mail to be delivered to PerfectMail™ from a remote server and there is no activity listed in this log, then the remote server did not connect to PerfectMail™.

Maximum Display Lines

To ensure the interface works smoothly, this screen limits the number of lines displayed to *Max Display Lines*. If this is not sufficient, modify your selection criteria as needed. *Max Display Lines* does not apply to downloaded data.

Download

Max Display Lines does not apply to transmission log file downloads. When downloading, be aware that log files can grow quite large. (Possibly hundreds of megabytes of information.)

Search Criteria

The log files can be quite large, so it's best to narrow your search as much as possible. Dates are formatted Year-Month-Day as YYYY-MM-DD.

You can also search for strings in the log files. Searching is done progressively, so all *search words* must appear in a line for it to be selected. You may group words as phrases by placing them between quotation marks (").

Selection by Message ID

The *Message ID* for each log line is highlighted as a blue *web link*. Clicking on a *Message ID* will present only the log lines pertaining to that message. (Clicking a second time will change back to the original search view.) A *View Message* button will appear if the selected message exists in the message archive.

(Note: PerfectMail uses *sendmail* as its MTA.)

13.4.3.1 Transmission Log Format

The raw log displays e-mail transmission information in multiple lines as a comma-delimited list of variable=value data elements.

```
date host sendmail[pid]: qid: var=value, ...
```

Example:

```
Aug 17 09:59:56 perfectmail sendmail[9999]: o7HDxtNY019999: from=<>, size=0, class=0, nrcpts=1, msgid=<201008171
Aug 17 09:59:56 perfectmail sendmail[18892]: o7HDxtNY019999: to=pmcheckstat@localhost, delay=00:00:00, pri=30000
```

Each e-mail transmission will record multiple log entries for different steps in the e-mail transmission. Click on the *message ID* of a particular message to display only that message.

The following log line elements are of particular interest:

- **class=** The queue class
- **delay=** Total time to deliver
- **from=** E-mail envelope sender
- **msgid=** The Message-ID: identifier
- **nrcpts=** The number of recipients
- **pri=** The initial priority
- **proto=** The protocol used in transmission
- **relay=** The remote host that sent or received the message
- **size=** The size of the message
- **stat=** Status of delivery
- **to=** The final recipient

13.4.3.2 Important Transmission Log Data Elements

Following are data elements that are particularly useful in diagnosing e-mail delivery problems.

delay=

The total amount of time the message took to be delivered. Note that the delay= equate is shown only for recipient records.

from=
The *envelope sender*. This may be different than the address in the *From:* header.

to=
The *envelope recipient*. This may be different than the address in the *To:* or *CC:* headers.

msgid=
A unique *message ID* is created for each e-mail on each mail server it passes through. This is very important for tracking messages. Each mail server should list the local *message ID* it assigns to the e-mail, reported in the *Received:* e-mail headers; however, not all e-mail servers do this.

nrcpts=
Number of recipients.

relay=
The hostname and network address of the remote host that either sent or received this message. For local e-mail submission the login name of the sender will appear in this field.

stat=
Delivery status. This is the **most important** piece of information in the log file. The *stat=* contains data that was reported by the remote mail server. In other words this is what the *relay=* server said in response to your e-mail transmission. If there is a problem with transmission, the remote server will often say what the problem was in this field. The remote server may also report the unique *message id* it has assigned to this e-mail transmission; which you can use to help diagnose problems when communicating with the mail administrators.

When diagnosing problems with e-mail transmissions it is very helpful to be able to say to remote e-mail administrators, *"At such and such a time **your e-mail server** identified by **this hostname** reported **this status message** for a message identified by **your local message id**. Why?"*

13.4.3.3 What is the *Milter (pm): to error state* message?

PerfectMail is implemented using an integration interface called *Milter* to our *Sendmail* message transport agent. Spammers will often connect to your PerfectMail server but close their connections, they leave them open. When the connection times out it is dropped and the communication between *PerfectMail* and *Sendmail* is interrupted. This interruption creates the *Milter (pm): to error state* message in the Transmission Log.

This is normal behavior and should not cause any concern, unless it appears on every message. In that case, the PerfectMail service may have stopped. In that case, restart the PerfectMail service using the dashboard.

FYI: PerfectMail has an independent process called *pmCheck* that looks for any problems with services and configurations. If it finds an issue, pmCheck will fix the problem and restart any services as required.

13.4.4 E-mail > By Domain

The PerfectMail™ e-mail activity search engine.

The *Mail Log*, *E-mail Activity*, *E-mail Search* and *Discovered Users* views display e-mail messages in a variety of ways. These screens display *e-mail messages* in a message-centric way. This is different than the *Transmission Log* view which displays e-mail transmission information. Use the *Transmission Log* to diagnose problems with *e-mail transmission* and the views above to diagnose problems with *e-mail disposition* and *filtering*.

Use the e-mail activity drill down screens to easily browse e-mail activity in an intuitive manner.

This page gives you the ability to query e-mail activity from a number of perspectives:

- **Server Summary** - Showing activity for each domain protected by the server.

- **Domain Summary** - Showing activity for each e-mail address in a domain.
- **E-mail address Summary** - Showing activity for a specific e-mail address.
- **Detail List** - Detailing individual e-mail messages.

Driving the page:
This page has a variety of options to change the way it's presented. Click on column headers to change the sorting. Click on the *server name*, *domain names*, and *e-mail addresses* to change the scope of your search. Also, you can make use of the *text search* feature to narrow down your search or restrict detail searches to a specific date range.

Changing views:

- The *summary view* displays statistical information. You can see the summary as either a *graphic report* or *text report*. Change your view using the link under the page title at the top right of the web page.
- The *list view* displays each e-mail described by the summary view. You can change between *summary* and *list* views using a link at the bottom right of the web page.
- Filter the *list view* by *showing* or *hiding* spam using a link at the bottom left of the page.

E-mail Content:
The *subject line* of each e-mail is actually a link to a pop-up window that displays the actual message content. However, the link is active only if the message content is still available in the message store; identified by a *blue* subject line and the presence of the *envelope icon*.

13.4.5 Activity > E-mail Search

E-mail searching is available in all e-mail activity query pages.

This form allows you to quickly search the *PerfectMail™ e-mail activity search engine*. Two types of searches are available:

- **Search by address and date** - PerfectMail tracks activity for protected e-mail address by specifying your tracked/discovered e-mail address. You can also specify a date range, to display the specific results close to your desired information. The date range has to follow the PerfectMai date field format which can be referred to by clicking on the **'?'** sign.
- **Search by Message ID** - Each e-mail message is assigned a unique *Message ID*, which is displayed in all error messages and the *message display* screen as well as the raw log files. Use the *Message ID* to jump to a specific e-mail.

13.4.6 E-mail > Mail Log

The *Mail Log* page presents a *list view* of all e-mail activity recorded in, and an entry point to, the *PerfectMail™ e-mail activity search engine*. Please refer to the "E-mail > By Domain" page for more information.

13.4.7 Activity > Discovered Users

The *discovered users* page lists all e-mail addresses that your PerfectMail™ product is currently tracking e-mail for. This page is an entry point into the *PerfectMail e-mail activity search engine*. Please refer to the *E-mail Activity* page for more information.

13.5 Quarantines = E-mail Uncertainty

A *quarantine* is a holding area for e-mail. Anti-spam filters use quarantines when they cannot decide what to do with an e-mail. This creates a problem of **E-mail Delivery Uncertainty**. The anti-spam solution is uncertain about the *disposition* of the e-mail (spam or legitimate?) and the sender and recipient are uncertain about the delivery of the e-mail.

"Where is my e-mail from ... ???"

"Why did ... not receive my e-mail???"

Because *PerfectMail™* is a *live filtering* solution it eliminates the problem of e-mail uncertainty. If PerfectMail accepts the e-mail, it is delivered. If PerfectMail rejects the e-mail, this is done during message transmission - **guaranteeing** the sending server receives the reject status, which is then passed to the sender.

Requiring users to check a quarantine for messages is a false economy. The user still needs to review their spam messages and they may have to do it using a separate application or website! All the quarantine has done is added a layer of complexity to checking e-mail. **Many users will not check their personal quarantine - EVER.** Messages held there are forever lost.

Rather than a *quarantine* which only reports spam, *PerfectMail* offers full *E-mail Activity Reporting* and a *Self Service Console*. We call this *User Empowerment*.

13.6 E-mail Recovery

Rather than having a *quarantine*, PerfectMail™ has a short term message storage facility where it keeps a copy of **all e-mail** that has passed through it, including a copy of most of the e-mail that PerfectMail *rejected*.

Not only can you release messages that may have been inadvertently rejected, but you can also resend messages that may have been lost for some other reason.

In fact, if you lose your *whole mail server* you can recover your e-mail by using the *Message Replay Wizard* to simply re-transmit any lost e-mail activity.

If your mail server does stop functioning, PerfectMail will identify and spool up your e-mail and automatically forward it to your mail server when it comes back up. Then, if necessary, you just replay the lost time period. Easy!

13.7 Reporting Spam to PerfectMail for Analysis

```
spam@perfectmail.net
```

If you see a trend in the spam coming through your server, please forward it to spam@perfectmail.net. We are constantly responding to trends. Often spammers are using techniques that are very difficult to identify with traditional content filters. This sort of feedback is very important to us.

Occasionally, industrial spammers will behave in a way that is legally legitimate; making it legally difficult to add them to Block Lists. These machines look legitimate and send content that looks legitimate, or at least not spammy enough to block. These are the types of messages we really want to see.

14 User Empowerment: Activity Report and Self Service Console

Rather than having a *quarantine*, PerfectMail™ has a short term message storage facility where it keeps a copy of **all e-mail** that has passed through it, including a copy of most of the e-mail that PerfectMail *rejected*. These stored messages can be viewed and managed using the *Administrator's Web Interface*.

We also offer tools that allow end-users access and management capabilities of their personal e-mail activity via the *E-mail Activity Report* and the *Self Service Console*. We call this *User Empowerment*.

We recommend enabling these features for a few users at first. Then add specific users as needed. Power users and sales people will probably appreciate these features. We also recognize situations where an executive assistant may use this as a tool for managing their executives e-mail. Or for allowing managers to monitor e-mail if the need arises.

14.1 E-mail Activity Report

The *E-mail Activity Report* is an e-mail based activity report, similar to the *E-mail Mail Log* on the *Administrator's Interface*. It shows a digest view of e-mail activity for a user. The report is typically sent once a day, though the *PerfectMail Administrator* can run the report multiple times through the day.

The E-mail Activity Report allows users to review their e-mail activity, with options to manage their e-mail directly from the e-mail client, or by clicking through to use the web-based Self Service Console. The report contains various action icons allowing users to view, release and resend messages, as well as allowing users to report spam to both your server and our spam clearing house for analysis.

Weekly and monthly reports are scheduled by week day (e.g. Monday, Tuesday, etc.) They run on the first *report hour* scheduled for that day. Monthly reports run on the first occurrence of the specified *week day* of the month. For example, for settings of *08:00* and *Monday*; a weekly report would be sent at 08:00 each Monday and a monthly report would be sent at 08:00 on the first Monday of the month.

14.2 Self Service Console

The *Self Service Console* lets users log in directly to the PerfectMail web interface using their e-mail address. The console gives users a web page showing their e-mail activity, giving them the ability to view messages, release/resend messages and report messages as spam. A link to the Self Service Console is included in the *E-mail Activity Report*.

There are two web pages available on the Self Service Console: *Activity* and *Settings*.

The Activity page displays the same information as the Activity Report, but in a more interactive medium. Users can search, view, release/resend, and report messages as spam.

The Settings page allows users to update some formatting and message inclusion features of the Activity Report.

The Self Service Console uses the same login screen for PerfectMail administration. Users log in using their *full e-mail address* and password. The default password is a random hash automatically generated by PerfectMail for use with the Activity Report. Users can specify their own password using the Settings page. If users don't have *one-click* access or if the Activity Report is not in use, then the administrator will have to assign passwords for each user using the *Domain Admin* page.

15 Training PerfectMail

As PerfectMail™ is mostly self-tuning, there are few tuning chores to distract administrators from their other duties. In fact, most PerfectMail products are run lights out (without administrator involvement) after their first week of service.

PerfectMail's inherent accuracy is enhanced by its embedded reputation system. PerfectMail's reputation system helps ensure the highest overall accuracy (typically better than 99.9+% and zero false positives). PerfectMail auto-discovers protected e-mail users and peers as well as legitimate and malicious mail servers. It watches live activity to make the best overall decision.

Let PerfectMail watch your e-mail traffic, both inbound and outbound, for about a week. After that use the *web interface* to review how your messages have scored. Look at the messages that score around your reject and tag thresholds. After about a week you can start lowering these thresholds. Lower the scores by about 2 points. Depending on your traffic, this will have a huge impact on the amount of spam that comes through your system. Then for the following couple of weeks perform this exercise again, dropping the scores 1 or 2 points, watching for any false rejects, until you find an acceptable setting.

15.1 Threshold Values

Administrators must assign values for the *Tag* and *Reject* thresholds for each domain protected by PerfectMail. It is common practice to start with higher values, to ensure no false positives (legitimate mail rejected as unwanted) and then adjust values down over time. Higher initial values will allow some amount of unwanted e-mail (spam) to sneak in under the *Tag* and *Reject* thresholds. Over time, reduce these to safe long-term values for *Tag* and *Reject* thresholds.

PerfectMail's reputation system will learn your users and their peers within a few days to a few weeks of service. Because PerfectMail strongly favors users and peers with an established reputation, it is safe to reduce *Tag* and *Reject* thresholds without the risk of introducing false-positive scores.

Optimal settings need to be determined empirically because each PerfectMail interacts with a unique set of users, mail peers and mail servers. To assist you, we suggest the following settings based on our own experience with the product:

	Tag	**Reject**
Initial Deployment or for each new Domain	16	26
Retail ISP and non-business settings	14	24
Safe long term settings	12	22
More aggressive long term settings	11	18

Note that scores have no meaning other than to indicate the magnitude of suspicious or undesirable activity discovered within a message. The overall range of scores that you might encounter is -50 or less for messages between peers with well established history, to 50+ for messages from one-time senders of strongly objectionable content.

15.2 Retail ISP Settings

Safe long-term settings for ISP's and organizations that dealing with a mix of business and non-business traffic need to be set a little higher than for traditional business. If your user population is primary non-business (e.g.: a retail ISP), then you might want to try 14 & 24. For organizations that use e-mail as a business tool, slightly lower settings (perhaps 12 and 22) may be more effective.

15.3 Safe Long Term Settings

Our experience indicates that many domains are well protected with Tag and Reject thresholds set to 12 and 22 respectively. At these values, users will receive relatively few unwanted messages (perhaps no more than one or two a day) with minimal risk of PerfectMail mishandling a message.

15.4 Aggressive Long Term Settings

Organizations that use e-mail as a business communications tool, and who exchange e-mail with other organizations that follow best-practices in the setup and administration of e-mail servers may find they can achieve even higher accuracy with no unwanted rejects by using slightly more aggressive settings.

If your organization fits this description, you might want to consider setting your **Tag** and **Reject** thresholds to 11 and 17 respectively.

Note: Do not reduce the Reject threshold below 11 without performing a thorough investigation to ensure that lower settings are safe for your organization. Our experience shows that some amount of e-mail, particularly from legitimate first-time senders may score up to 12. Use low Tag values only if you don't mind first-time messages receiving the [SPAM?] marker on their subject line or you choose to hide the [SPAM?] marker.

15.5 Reviewing E-Mail Scores

Before adjusting PerfectMail's domain scores you should take some time to review the mail activity on your appliance so that you can establish safe Tag and Reject settings for your system.

PerfectMail provides a real-time, interactive query and reporting facility that lets you examine your e-mail history. To perform any PerfectMail query, log into the web interface by pointing your web browser at the fully qualified domain name or IP address of your PerfectMail server. You will need to log in with a pre-established account name and password. By default, PerfectMail ships with an account named admin, password admin (although the password should have been changed during the initial installation).

Since most servers receive much more legitimate e-mail traffic than Rejected traffic, it makes sense to click the Score column header to sort descending.

Make a note of the highest score of the first e-mail message that should not obviously have been rejected. This score plus 1 or 2 is a good candidate for your new system-wide default Reject threshold.

15.6 Applying New Thresholds

Using the information gathered from your e-mail history, adjust the *Tag* and *Reject* thresholds for each of your domains in the "Domain Admin > Domains" page of the *web interface*.

Continue to periodically review e-mail and adjust these thresholds as required.

16 PerfectMail™ Updates and Upgrades

PerfectMail is an actively developed product with regular releases to rules, signatures, block-lists and code updates.

Updates: Updates to *PerfectMail* occur on a regular and ongoing basis. Your server will check for updates to its spam and virus settings every 10 to 15 minutes to quickly adjust how it reacts to spam threats.

Upgrades: Periodic code releases are made to add more tools or make improvements to our anti-spam engine.

16.1 The Upgrade Process

We provide a 72 hour post install support availability window, where staff must be available to deal with any upgrade issues.

The upgrades themselves occur seamlessly on your PerfectMail™ server. The latest upgrade is downloaded to your server; after which mail services are suspended and the upgrade is applied. The total downtime is usually about 30 seconds, with no loss of e-mail.

After the upgrade is finished your PerfectMail™ server will send you an e-mail notification.

16.2 Staggered Upgrade Scheme

We have a staggered upgrade release schedule to minimize any disruption to your Mail Server. Prior to general release PerfectMail is tested on our Development, Alpha and Beta sites. After successful deployments through these three server groups it becomes available for general release, being pushed to upgrade groups: 'A', 'B' and 'C' in a progressive release schedule.

'A' sites receive their updates on the Monday of the general release; 'B' and 'C' sites receive their upgrades later in the week, or even in the following week.

At any time, if there are any reported issues they are assessed and appropriate actions are taken.

17 E-Mail and Anti-Spam Concepts

17.1 What is SMTP?

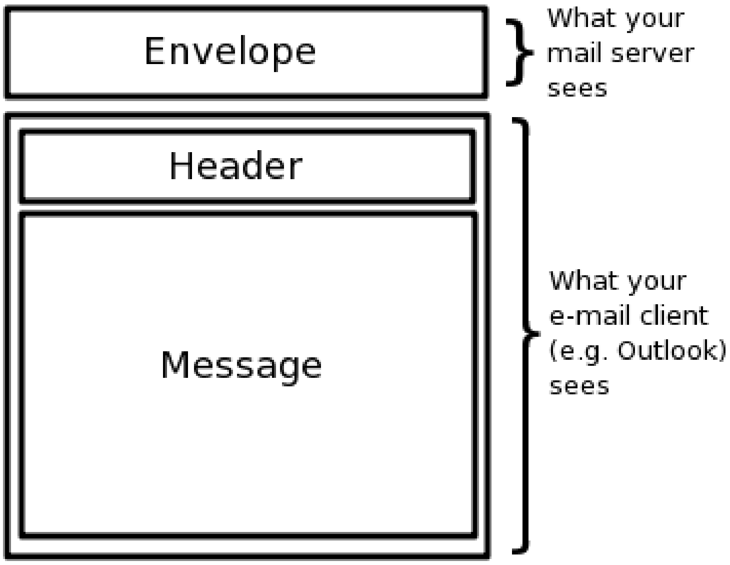
SMTP (S M T P) stands for *Simple Mail Transfer Protocol*. It is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP.

SMTP is commonly used to send messages from a mail client to a mail server (i.e. sending from a mail client application like *Microsoft Outlook™*.) The new protocol for mail submission (MSA) is essentially the same as SMTP, but it uses port 587 instead. (This new standard is slowly being adopted.)

SMTP was first defined by RFC 821 (1982, eventually declared STD 10),[1] and last updated by RFC 5321 (2008)[2] which includes the extended SMTP (ESMTP) additions, and is the protocol in widespread use today. SMTP uses TCP port 25.

17.2 E-mail Structure

E-mail is actually composed of two main elements: the *envelope* and the *data* sections. The *data* section is further divided into the e-mail *header* and e-mail *body* or *message*; which may be comprised of different alternative formats and contain embedded images and other elements; as well as e-mail *attachments*.


Envelope
What your mail server sees
Header
Message
What your e-mail client (e.g. Outlook) sees

If we focus on the two main elements, the *envelope* and the *data* sections you can think of an e-mail like a conventional written letter.

The *envelope* contains addressing and delivery information. Your e-mail server uses the *envelope* to decide how an e-mail should be forwarded or delivered. It ignores the actual *message*.

When you view an e-mail using your mail App (e.g. Microsoft Outlook™), you are seeing the *data* section comprising the *header* and actual *message*; the envelope has been stripped away. Liken this action to a receptionist who has taken the letters from their envelopes, put those letters on your desk and discarded the envelopes.

17.3 E-Mail Addresses and Delivery

The *envelope* is used, and only used, for message delivery, just like a written letter.

The e-mail *header* is made up of what we like to think of as the delivery information: the From, To, Subject, Date, etc. But this simply is not the case. The delivery information is contained in the *envelope*, which has been discarded. The *header* information is simply information displayed as a courtesy to the recipient.

The information in the *envelope* and the *header* are completely unrelated! For legitimate messages the *header* will contain the original delivery information, but this is simply not something that is enforced.

17.4 Envelope Abuse

Spammers make use of the inconsistency between the *envelope* and the *header* to try and side-step spam filters. They do many things to push the boundaries of what is acceptable in e-mail. This is why you can receive emails that look like they were addressed to someone else, or no-one at all. In fact, you can put any e-mail address in the *header*!

So why don't we just block this sort of e-mail? Unfortunately, many legitimate e-mail clients also push the boundaries of what is acceptable in e-mail and the spammers take advantage of these issues. Also, this technique is commonly used by distribution lists and newsletters. You may often see text such as "undisclosed-recipients". This technique is so widely used that we cannot block these sorts of messages.

(PerfectMail™ adds a score for mismatches between the e-mail *envelope* and *message headers*, but this alone is not enough to reject a message.)

17.5 Anti-Spam Tests

PerfectMail™ uses a variety of anti-spam tests:

- Sender Reputation
    - ♦ Real-time Block Lists
    - ♦ Incoming Sender Lists (Black/White lists, etc.)
    - ♦ Real-time dynamic sender behavior analysis
- Historical Information
    - ♦ Past server and sender behavior
    - ♦ Analysis of e-mail traffic patterns
- Server Analysis
    - ♦ Sending server analysis
    - ♦ Sending address verification
    - ♦ DNS configuration validation
    - ♦ Server profiling and identification
- Sender Intention Checks
    - ♦ Test for sender/origin obfuscation
    - ♦ Phishing attempt identification
    - ♦ Recipient validation
    - ♦ Spam Traps
- Content Scanning
    - ♦ Anti-virus scanning
    - ♦ Dangerous attachment filtering

- E-mail structure analysis
- Content black listing and watch words
- Anti-obfuscation engine
- OCR analysis
- Adaptive content filtering

17.6 Static Content Filtering

17.6.1 Black and White Lists

Use Black and White Lists when other methods are not working. White listing can be an effective method for ensuring mail deliver. Black Listing however, is only useful for persistent spammers.

Occasionally, industrial spammers will behave in a way that is legally legitimate; making it legally difficult to add them to Block Lists. These machines look legitimate and send content that looks legitimate (or at least not spammy enough to block.) Often the best way to block these spammers is to make use of Black Lists. (Though we're working on some techniques to block them as well... coming soon!)

17.7 Dynamic Content Filtering

Spam can be identified by server reputation, validation, best practices, history and message content. Message content is the least useful tool in blocking spam. Your PerfectMail™ appliance is constantly self training on new content to catch questionable messages. However, there are some things you can do to help this process.

17.7.1 Local Dynamic Content Filtering

```
SPAM@ and HAM@
```

Your PerfectMail appliance uses a custom Bayesian content filtering solution to help identify content trends in Spam.

To help train the Bayesian filter, forward your spam to a special "spam@" address on your PerfectMail server. For example: if your appliance has the host name perfectmail.mydomain.com, forward your spam to spam@perfectmail.mydomain.com. (Naturally your DNS, host tables, etc. must be configured to resolve this address.)

Similarly, from the above example, you can forward legitimate e-mail to your PerfectMail™ product as well, by forwarding mail to ham@perfectmail.mydomain.com.

Our clients will often create e-mail aliases on their mail servers to make forwarding e-mail easier for their users. Create aliases such as:

```
spam@mydomain.com => spam@perfectmail.mydomain.com
ham@mydomain.com => ham@perfectmail.mydomain.com
```

17.7.2 Heuristic Analysis

Heuristic Analysis is a process where a message is analyzed for various qualities that identify it as particular type of spam, possibly with a particular type of message. These techniques allow PerfectMail to quickly react to a changing attack patterns by regularly updating heuristic profiles using our central data services.

17.7.3 Bayesian Analysis

Our *Adaptive Bayesian Engine* dynamically calculates the probability of message being spam based on its contents using a probability model.

Our adaptive engine self trains using sample messages from known spam sources and known valid e-mail traffic. This allows us to automatically analyze **your** e-mail traffic in **Real Time**.

Localized adaptability is very important. While for most people spam may have similar characteristics, each site's legitimate e-mail may be quite different.

17.7.4 PerfectMail Block List™

The PerfectMail Block List™ (PMBL) is maintained by PerfectMail™. This is a fast turn-around database of computers that are currently attacking the PerfectMail Anti-Spam Grid™.

17.7.5 Spamhaus Block List

The Spamhaus Block List (SBL) is maintained by a dedicated international team based in eight countries, working 24 hours a day, 7 days a week.

PerfectMail uses the Spamhaus RBL list because it is a high quality, well researched and well maintained list. If you end up on Spamhaus' list, you really do have a problem with your site sending spam.

17.7.6 Exploits Block List

The Exploits Block List (XBL) is a real-time database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, Socks, AnalogX, Wingate, etc), worms/viruses with built-in spam engines, and other types of Trojan-horse exploits. There are two subgroups within this feature:

XBL (CBL) - Composite Block List

> The CBL takes its source data from very large spam traps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, Socks, AnalogX, Wingate etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of Trojan-horse or "stealth" spam ware, without doing open proxy tests of any kind. (See cbl.abuseat.org)

XBL (NJABL) - Open Proxy IPs List

> This service performs automated open relay and open proxy tests against any system that connects to any of the SMTP servers on networks that contribute relay data to the list. (See www.njabl.org)

17.7.7 Policy Block List

The PBL is a database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use. The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges.

PBL IP address ranges are added and maintained by each network participating in the PBL project, working in conjunction with the Spamhaus PBL team to help apply their outbound email policies.

Additional IP address ranges are added and maintained by the Spamhaus PBL Team particularly for networks which are not participating themselves (either because the ISP/block owner does not know about, is proving difficult to contact or because of language difficulties) and where spam is received from those ranges, reverse DNS (rDNS) and server patterns are consistent with end-user IP space which typically contain high concentrations of "botnet zombies", a major source of spam. Once aware of them the ISP/block owner can take over such records at any time to manage them further.

The PBL lists both dynamic and static IPs; any IP which by policy (whether the block owner's or -interim in its absence- Spamhaus' policy) should not be sending email directly to the MX servers of third parties.

A feature of the PBL is the elimination of 'false positives' with a server-identifying and automatic removal mechanism for single IP addresses. This allows end users with static IP addresses within a larger dynamic pool and legitimate mail server operators, to assert that in their opinion their IP addresses are a trustworthy source of email and to automatically remove (suppress) their IP addresses from the PBL database. Safeguards are built in to prevent abuse of this facility by spammers (and particularly by automated bots).

Servers blocked by the PBL service will receive a "PBL Block" error.

Home based e-mail servers may be blocked if their ISP has stated their IP address should not be sending e-mail. Be aware of this.

17.7.8 SURBL

SURBL is a collection of URLs or links that are commonly referenced in "spamvertizer" messages and phishing attacks. These URLs can either be pointing to a page on the spammers website or for referencing images or other content from the spammers website. The mail body is parsed for URLs or links and these links are queried against various URL reputation services.

The URLs are harvested from a variety of anti-spam networks. Each spam filtering technology has specific spam it is strong in stopping. Combing the lists makes for a more effective filter. Some of the sources are:

- PerfectMail™ sites
- Phishing and Malware sites
- Spam Assassin sites
- SpamCop sites
- AbuseButler sites
- Outblaze URI Blacklist
- jwSpamSpy and Prolocation sites

17.7.9 Drop List

DROP (Don't Route Or Peer) is an advisory "drop all traffic" list, consisting of stolen 'zombie' net-blocks and net-blocks controlled entirely by professional spammers.

The DROP list will NEVER include any IP space "owned" by any legitimate network and reassigned - even if reassigned to the "spammers from hell". It will ONLY include IP space totally controlled by spammers or 100% spam hosting operations. These are "direct allocations" from ARIN, RIPE, APNIC, LACNIC, and others to known spammers and the troubling run of "hijacked zombie" IP blocks that have been snatched away from their original owners (which in most cases are long dead corporations) and are now controlled by spammers or net-block thieves who resell the space to spammers.

This list is implemented automatically on PerfectMail™. Senders from such networks will receive a "Drop List" reject message.

18 Frequently Asked Questions

What Anti-Spam services does PerfectMail offer?

PerfectMail provides comprehensive anti-spam and anti-virus services for protecting enterprise e-mail systems from spam, viruses and other types of e-mail borne attacks. Our web-based administrative console and web-based reporting features allow administrators to effectively manage their e-mail systems, regardless of server vendor type, hardware platform or location.

Is PerfectMail compatible with my mail server?

Yes. PerfectMail is 100% compliant with SMTP standards and will work with any Internet Mail Server.

Does PerfectMail require extensive integration with existing systems?

No. PerfectMail, either as a server-based solution or a managed service, operates as a separate entity requiring minimal integration.

What delivery models does PerfectMail use in offering its product?

PerfectMail can be delivered as a server based solution or as a managed service. We provide a full server install ISO image that you can install on your local hardware or as a virtual appliance. We also offer a fully managed service at our Class A datacenter.

How do I implement PerfectMail as a managed service?

Simple DNS updates redirect incoming e-mail messages to flow through the PerfectMail servers at our Class A datacenter, for real-time filtering before delivery to an end-users inbox. Spam and virus-infected messages are then either filtered at the server or scored and forwarded for desktop level filtering.

What types of anti-spam technology does PerfectMail use to filter spam?

PerfectMail's anti-spam engine was developed 100% in house using our own technology that utilizes heuristics and adaptive algorithms to check content, structure, history, reputation and references; and other information extracted from e-mail messages.

Does PerfectMail processing delay message delivery?

Unlike "store and filter" spam solutions, PerfectMail filters e-mail in real-time (literally within milliseconds). There will be no noticeable delay in mail delivery.

How many domains can I protect with PerfectMail?

The number of domains you can protect is restricted by your PerfectMail license type. The Advanced and Enterprise Editions of PerfectMail have unlimited licensing on domains. We have customers who host over a thousand domains on a single PerfectMail server.

How many mail servers can I protect with PerfectMail?

PerfectMail has no restrictions on the number of mail servers that can be protected. PerfectMail can protect as many mail servers as there are domains you are hosting.

How many e-mail addresses can I protect with PerfectMail?

PerfectMail has no restrictions on the maximum number of e-mail addresses that can be protected on any license. However, there are limitations based on the number of concurrent e-mail connections your license will allow. This effectively sizes PerfectMail, based on license, for different types of organizations. Choose a PerfectMail license that is appropriate for your organization and forget about license compliance based on the number of users or e-mail addresses you support.

Can PerfectMail handle large outbound e-mail blasts?

Yes. Many of our clients relay their outbound newsletter and marketing messages through their PerfectMail servers. In fact, sending your e-mail blasts through PerfectMail helps to build e-mail history with your marketing and newsletter recipients to help reduce false positives when filtering incoming e-mail.

Will PerfectMail appliances crash under excessive load?

No. PerfectMail appliances limit the number of concurrent messages they handle to fit within the capabilities of the server hosting PerfectMail. Excess e-mail connections are refused until the server load drops to an acceptable level.

Does PerfectMail have any way of defending against a Distributed Denial of Service Attack (DDOS)?

Yes. PerfectMail has strategies in place to defend against various types of focused and distributed SMTP based attacks. PerfectMail maintains a database of "known servers" for which it reserves a minimum number of e-mail connections. This number adjusts depending on the number of mail connections received from "known servers". In a DDOS situation "unknown" mail servers and "known" mail servers are each allotted a number of e-mail connections with preference being given to "known" mail servers. This guarantees that server resources are given to "known" mail servers effectively mitigating the effects of a DDOS attack.

What type of anti-virus technology does PerfectMail use to filter viruses?

PerfectMail incorporates the ClamAV anti-virus engine, designed for detecting Trojans, viruses, malware and other malicious threats. It is the de facto standard for high performance mail gateway scanning.

How often does PerfectMail update its virus database?

PerfectMail includes an intelligent tool for automatic signature updates, checking for updates every 10 minutes, to ensure your virus signatures are always up to date.

What does PerfectMail do with e-mails containing viruses?

When PerfectMail identifies a virus or other dangerous e-mail attachment it rejects the message outright, during the SMTP transaction. PerfectMail responds with an SMTP reject code which will be returned to the sender stating that the message was rejected because it contained a virus (or dangerous attachment) with details on the virus (or dangerous attachment) that was found.

Our company already has an anti-virus solution that includes spam filtering. Does that make PerfectMail redundant?

While many organizations have been able to manage their virus problems using current anti-virus tools, the high volume and variability of Spam and other e-mail borne attacks present an ever increasing security problem. PerfectMail anti-spam provides industry leading technologies not available in anti-virus products that can easily work in conjunction with existing anti-virus solutions. The best defense against spam and viruses is a multi-layer defense: Spam and anti-virus defense at the perimeter with PerfectMail, anti-virus defense at the mail server and spam (and possibly anti-virus) defense at the desktop.

Our company already has anti-spam filtering at the desktop. Why do we need PerfectMail?

Spam is an ever evolving, dynamic and increasing problem, requiring ongoing development and attention that is difficult to implement at the desktop level. PerfectMail anti-spam provides industry leading technologies not available in desktop filtering tools, providing excellent spam filtering with extremely low false positive rates. Further, PerfectMail can easily work in conjunction with desktop spam filtering to provide a spam filtering solution that is both extremely effective and easily manageable for end-users.

How do I release blocked spam messages or recover lost e-mail?

All e-mail, including both spam and legitimate messages are stored on the server for a short period of time; typically 14 to 30 days. (Types of spam and holding time is dependent on individual server settings.) A web-based administrator interface gives administrators full access to review, release, resend and report all e-mails - both spam and legitimate messages. E-mail Activity Reports and a Self Service Console are also available to give end-users the ability to manage their e-mail without burdening mail administrators with excessive support requests.

Is PerfectMail PCI compliant?

Payment Card Industry (PCI) compliance does not apply to a particular technology element within an organization; rather it reflects the state of the organization itself. PerfectMail can be part of your PCI compliant e-mail system. PerfectMail anti-spam is an edge-device supporting TLS encryption, allowing for the sending and receiving of secure data across public networks using the SMTP protocol. Using HTTPS, administrators can also manage their PerfectMail server in a secure manner. Review the PCI compliance guidelines and take the necessary precautions with the setup and configuration of your PerfectMail appliance to ensure PCI compliance.

Does PerfectMail use Active Directory?

PerfectMail does not use Active Directory for e-mail address validation. Rather, it makes use of the SMTP Recipient Filtering setting in Microsoft Exchange to extract that information from your Exchange server during e-mail transmission.

19 Troubleshooting Network Issues

19.1 Network Connectivity Diagnostics

How can I diagnose network connectivity problems with PerfectMail?

Network problems can be very annoying when they happen. PerfectMail™ provides a number of tools to assist administrators in diagnosing network connectivity issues. Available tools include:

- **DNS Lookup** - Used to perform DNS Lookups;
- **Ping** - Used to test network connectivity between PerfectMail and another network device;
- **TraceRoute** - Used to trace the network route between PerfectMail and another network device;
- **WhoIs** - Used to look-up human readable information about an Internet domain name;
- **SMTP Test** - Used to diagnose low level SMTP protocol exchanges between PerfectMail and another mail server.

Additionally, PerfectMail performs periodic diagnostics of its configuration and connectivity to local infrastructure and the Internet. PerfectMail displays the health of its DNS configuration, Network Status and Mail Server Status on the Dashboard. The detailed results of these diagnostic tests are available in the *Server Status Report*, "Reports > Server Status".

In e-mail diagnostics, first verify that network connectivity exists then check that DNS resolution is functioning correctly. Following is a step-by-step process to aid in general network diagnostics:

Step 1: Record local settings.

Confirm and record your local network settings under "Server Admin > Networking", including: IP Address, Gateway and DNS servers. If you are having problems with a specific mail server, record the IP address of the mail server.

Step 2: Test basic connectivity.

Confirm basic network connectivity using the *Ping Tool*, "Tools > Ping". Ping each device recorded in *Step 1* (Gateway Server, each DNS server and any Mail Servers.) Note: Some network devices, including firewalls, may disable ping packet responses or even block the ICMP protocol, used to send ping network packets.

If you are experiencing connectivity issues at this stage, use the *TraceRoute Tool*, "Tools > TraceRoute", to try and identify where the connectivity issue is located. Once again, firewalls and other devices may block the gathering of this information.

This step may identify a problem, or it may simply identify that your firewall is preventing you from gathering this information. If this is your situation, continue the diagnostic process keeping in mind connectivity issues may still be your problem.

Step 3: Confirm DNS resolution.

Confirm DNS resolution is functioning. Use the *DNS Lookup Tool*, "Tools > DNS Lookup", to verify DNS resolution is working. Perform DNS Lookups against each of your listed DNS servers for well known hosts (e.g. www.google.com). Also, perform queries for hosts which will likely note be cached by your DNS server. Confirm DNS responses with those returned by DNS servers external to your organization (e.g. 4.2.2.1, 4.2.2.2, 8.8.8.8, etc.)

Frequently DNS servers may appear to be operating correctly when tests are performed against DNS entries which may be cached, while new DNS queries may fail. (This sometimes happens with *Microsoft DNS services*; rebooting the service resolves this problem.)

Occasionally, if there has been a significant DNS outage the PerfectMail *Mail Transport Service* (MTA) may need to be restarted. If you are not receiving incoming e-mail from domains you expect to receive e-mail from, try restarting the MTA service using the following proceedure:

1. Log in to the PerfectMail web interface;
2. On the Dashboard, locate the Mail Transport Service (MTA) status at the top left of the screen;
3. Stop the Mail Transport Service, then start the Mail Transport Service.

Step 4: Confirm SMTP Connections.

If basic connectivity and DNS resolution are functioning correctly, there may be a problem with the actual SMTP exchange. Occasionally, we see problems where firewalls, ISPs, etc. will block SMTP (port 25) traffic. There may also be configuration issues where SMTP services are not running or address acceptance or routing is broken.

You can diagnose SMTP connections using the *SMTP Test Tool*, "Tools > SMTP Test". This tool allows you to specify a mail server IP address and port number, along with sender address, recipient address and simple content for testing purposes. The *SMTP Test Tool* will actually send an e-mail to the recipient you choose, directly through the specified mail server. During the process of sending this e-mail the actual SMTP commands used during communication will be displayed, along with any error messages.

19.2 DHCP Issues

If the network interface is configured for DHCP and a DHCP server is not available the network interface *will not start*! Check to make sure the network interface is configured correctly. You may need to log in to the system console with userid: **root** and password: **admin** to reconfigure an interface that will not start.

19.3 Server Has A DHCP Lease, But Should Be Static

If your server has a DHCP lease, but you have configured it with a static IP address, you likely have a duplicate IP on your network. Try to ping the IP address you were expecting. If it is on the network then you need to resolve the IP address conflict.

20 Trouble Shooting E-mail and Spam

20.1 Not Accepting Mail

PerfectMail™ may stop accepting e-mail for a number of reasons. Fortunately, PerfectMail runs a periodic validation script that checks for the most likely reasons and displays error messages and warnings on the *PerfectMail Dashboard*. It there is a problem with e-mail delivery, check the dashboard first.

20.1.1 Resolvable Hostname Issues

A server's *hostname is the name that it knows itself as. This is different than naming in DNS or any other mechanism. It is the locally defined name.*

Your PerfectMail product **must** have a *resolvable, fully qualified hostname*; e.g. `perfectmail.mydomain.com`. There **must** be a domain portion to the *hostname* of your PerfectMail server.

This *hostname* must be resolvable in DNS. Mail servers will look-up server names in DNS as a validation mechanism. Not having a resolvable *hostname* can cause problems.

If this is not possible to use resolvable DNS names you can use the `.localdomain` domain; e.g. `perfectmail.localdomain`.

The PerfectMail configuration scripts try to mitigate the creation of partial hostnames by appending all single word hostnames (e.g. "myhost") with the ".localdomain" top-level-domain (e.g. "myhost.localdomain"). The ".localdomain" top-level-domain is "known" and will not be validated against DNS.

20.1.2 Unique Hostname Issue

Your PerfectMail *hostname* must be unique. Often, mail servers will refuse to relay e-mail through mail servers with the same *hostname*. This is done to prevent endless e-mail delivery loops.

20.1.3 DNS Issues

PerfectMail absolutely needs to be able to perform DNS resolution. PerfectMail will refuse to accept e-mail from domain names that do not exist in the DNS space. If DNS is not resolvable then e-mail will not flow.

DNS is also used for a number of validation tests including look-ups on many RBL sites. Not having the ability to perform DNS look-ups severely impairs PerfectMail's ability to filter e-mail.

20.1.4 Server Resources

Memory constraints are the most likely cause of server problems. PerfectMail must have sufficient resources (i.e. memory, CPU and disk) to run. If the server uses all memory and swaps to disk the system performance will slow down significantly. If your server appears to be running slow, check the memory usage and add memory as appropriate.

If the hard disk becomes full PerfectMail will stop accepting e-mail. A nightly script prunes old data to ensure a safe amount of free disk to prevent this from happening.

When the "load average" of the server is greater than 12 (i.e. 12 processes waiting for the CPU) our Mail Tranpsort

Agent (MTA) will stop accepting new e-mail connections. This behavior prevents the PerfectMail server from crashing. With a high server load your server is not realistically able to process mail in any case as pushing the load average past 12 can put the server in an unresponsive state.

In any case, if your server is performing sub-optimally, you will likely need to review your resource usage and increase resources as appropriate. PerfectMail provides reports on its web interface to assist you with this assessment. Please refer to the following reports:

- "Reports > E-mail Activity"
- "Reports > Resource Usage"
- "Server Admin > Archive"

20.2 Server Has A DHCP Lease, But Should Be Static

If your server has a DHCP lease, but you have configured it with a static IP address, you likely have a duplicate IP on your network. Try to ping the IP address you were expecting. If it is on the network then you need to resolve the IP address conflict.

20.3 Why does an e-mail get *Deferred*

E-mail deferral occurs when a message (usually outgoing) cannot be immediately handed off to the next relay host. It is quite common to have messages queued as "deferred" as remote mail servers may not be available for any number of reasons: network traffic congestion, service outages, server load, DNS hiccups, grey-listing, etc.

Sometimes *spam* and *delivery notification messages* will get stuck in the queue as well. Spammers send a lot of e-mail, but rarely accept return e-mail, including bounce messages. These messages can get stuck in the queue. PerfectMail™ has automated processes that clean out such messages on an hourly basis.

20.4 My Outbound E-mail is RBL Listed!

There are many RBL services available on the Internet. If your mail server becomes listed by one of the RBL services you need to go to the website for that particular RBL service. Most RBL sites will provide a look-up page to check if your mail server is listed. Most will also provide a web page for de-listing your mail server.

It's unlikely you were listed without reason. Use the web-tools provided by the RBL site to find out why you were listed. Common reasons are:

- Your mail server has a configuration error that makes if vulnerable to attack.
- Your mail server has been hijacked by a spammer
- A PC in your organization has a spam-virus.
- Your users may be blasting out marketing e-mail that might get reported as spam
- Your server was listed in error.

Once you have solved the problem, visit the RBL service again and ask to have your mail server removed from their block list.

It's important to fix any problems. Repeated listings may find your server permanently listed with an RBL site.

A RBL reject message looks like this:

```
From: Mail Delivery Subsystem <mailer-daemon@recipientDomain.com>
Date: Nov 21, 2006 4:46 PM
```

```
Subject: Delivery Status Notification (Failure)
To: theSender@senderDomain.com

This is an automatically generated Delivery Status Notification

Delivery to the following recipient failed permanently:

    recipient@recipientDomain.com

         Technical details of permanent failure:
         PERM_FAILURE: SMTP Error (state 9): 550 5.1.1 <recipient@recipientDomain.com>... RBL Block:
         spamhaus.org 1.2.3.4
```

Note the IP address above. This is the IP address of the blocked mail server. SpamHaus is the only external RBL service PerfectMail uses. You can query SpamHaus directly by entering the following URL into a web browser (for the above example):

```
http://www.spamhaus.org/query/bl?ip=1.2.3.4
```

To see if you are listed in any of 250+ other popular RBL list sources, please try the following query:

```
http://www.dnsstuff.com/tools/ip4r.ch?ip=1.2.3.4
```

If your IP address is on SpamHaus' RBL lists, please follow the instructions on SpamHaus' web site to remove your IP address. Please keep the following in mind:

- It may take a day or more from the time you ask to have your site removed to the time your mail server is removed from a black list. Consequently, you need to act quickly to ensure minimal interruption to your e-mail service.
- Do not remove your site from a black list unless you are certain that you are no longer forwarding spam. Most black list sites have a 3 strikes rule. They will let you remove yourself 3 times without question. After that, you will have to prove that you are no longer a spam source.
- Mail servers, and antispam products, use many different black lists to determine if a message may be unwanted. Removing yourself from SpamHaus is necessary but may not be enough to fully unblock your server.
- Most mail servers use some sort of RBL protection. If you do not get your server off of popular RBL lists, you will not be able to send mail to most businesses and about 50% of the rest of the Internet.

20.5 A Spammer Is Using My E-mail Address!

E-mail is very prone to this sort of thing. When an e-mail is crafted, you can say you are anyone you wish! Spammers take advantage of this to give themselves more credibility and deflect bounce messages to other people.

The best way to block this sort of thing is using Sender Policy Framework (SPF). SPF is implemented as a DNS entry for your domain. It specifies what hosts are valid for sending mail for your domain. Any other host should be considered a hoax.

You can get more information on crafting an SPF Record by going to http://www.openspf.org/. On this page there is a section called "Deploying SPF", with a web form for crafting an SPF record (currently set to example.com). Use this to craft an SPF record for your domain.

Many e-mail hosts and even anti-spam filters are not making use of SPF records, so there will always be a number of false messages being delivered; but this is the best method available to us at this time.

20.6 Receiving e-mail not addressed to me

E-mail is actually composed of two elements. The envelope and the actual e-mail. Think of it like a conventional letter.

The envelope contains the addressing/delivery information. Your mail server looks at the envelope to decide where the e-mail should go, but will ignore the actual e-mail content. The actual e-mail content contains the e-mail headers (including From: To: Subject:, etc), message body and any attachments.

Your e-mail client displays only the actual e-mail content; the envelope has been stripped away. Liken this to a receptionist taking your letters from their envelopes, putting those letters on your desk and throwing away the envelopes.

This is why you can receive emails that look like they were addressed to someone else or no-one at all. If you received the e-mail, then be assured your e-mail address appeared on the envelope.

Why don't we just block all of this type of e-mail? Well, this technique is commonly used by distribution lists and newsletters. You may often see text such as "undisclosed-recipients". This technique is so widely used that we cannot block these sorts of messages.

20.7 Domain of Sender Does Not Exist

Someone tried to send me a message and received the following response:

```
SMTP Error 553 5.1.8... Domain of sender address does not exist
```

What does this mean?

In this situation, your mail server has refused the e-mail because it cannot identify the sender's domain (e.g. example.com) as a valid registered domain name. This is a common practice across most mail servers.

There may be a problem with the senders domain. More likely, there may be a DNS issue at your site.

Sometimes this sort of thing occurs when domains are moved from one ISP to another. You can get an inconsistent view of DNS where the Internet as a whole has one view of DNS, while a particular ISP (and all it's clients) get another view.

I recommend speaking with your technical support team. Get them to see what happens if they try DNS resolution for the senders domain on their e-mail server.

Also, this may have been a temporary issue that has since been resolved. If that's the case the technical support team won't see anything wrong. Try sending the message again to see if the issue has been resolved.

20.8 Why am I still receiving Spam?

There are a number of reasons why the amount of Spam you receive does not go down immediately after activating PerfectMail.

Here are the most common reasons along with suggestions on how to fix the problem:

- You may be receiving e-mail from unprotected mail accounts. It is quite common for people to have multiple e-mail accounts. Modern mail clients (e.g.: Outlook) can poll for mail from many sources and consolidate it into a single in-basket. PerfectMail will block Spam from your protected accounts but not from unprotected accounts. If all of your e-mail accounts are on local servers, then you can solve the problem in one of 2 ways:
    1. Be sure that PerfectMail filtering is configured for all of your domains. To do this, create domain records in PerfectMail for all local mail servers and all of their respective domains. Be sure to indicate that each domain has filtering enabled (Domains > Your Domain > Filtering Enabled is checked).
    2. Ensure that all mail is directed to your PerfectMail server. This may involve updating DNS mail exchanger (MX) records so that they direct mail to your new PerfectMail server or changing the SMTP port forwarding rules at your firewall to direct all traffic to your PerfectMail appliance.
- You may be receiving e-mail from remote mail servers. PerfectMail can only protect e-mail traffic directed to local mail servers. Often people use a mix of e-mail accounts on both local and remote mail servers. PerfectMail cannot protect remote mail servers or popular Web based mail services like HotMail, MSN or Yahoo Mail.
- You may have insecure mail relays. PerfectMail can be told to accept all e-mail from a trusted source. If this trusted mail server also accepts mail from the Internet, then you are providing a back door through which Spam may arrive. To solve this problem, ensure that your internal trusted mail relays do not accept e-mail directly from the Internet. Stated another way, all internal relays must be outbound only mail relays, not inbound mail relays.
- Spammers may continue to use your old IP address. A common implementation strategy is to provide PerfectMail with a new IP address and then redirect e-mail to the new address via DNS MX record updates. This strategy works well for legitimate senders but may result in no immediate decrease in Spam.

  Our research has shown that Spam engines do not do DNS queries for each message they send. Instead, they query DNS once and then remember (cache) the answer - sometimes for months. Since DNS queries take time and mail servers rarely change IP addresses, caching IP addresses helps Spammers send out much higher volumes of junk mail.

  Often the old IP address is still a legitimate pathway to your mail server. If true, and spammers have cached your mail servers' IP address, then Spam will continue to show up in your inbox.

  You can solve this problem by migrating all of your domains to PerfectMail as quickly as possible. Once this is done, configure your firewall to shut down mail handling on the old IP address.

  Another solution is to configure your local mail server so that protected domains may only communicate with the mail server from the IP address assigned to PerfectMail (as that is their only legitimate pathway). The local mail server should not accept SMTP traffic for protected domains directly from the firewall.

20.9 A legitimate message was tagged [SPAM?]

PerfectMail prepends the phrase [SPAM?] to messages that score above the Tag threshold but below the Reject threshold. This is intended to indicate that PerfectMail was uncertain as to the real disposition of the message (wanted or unwanted) and so it chose to forward the message with a warning to the recipient.

There are a number of things you can do to address this situation:

- Nothing. PerfectMail will continue to watch your e-mail traffic and record activity between you and your senders. If a sender continues to e-mail you from the same location, with the same e-mail address, then PerfectMail will quickly recognize a 1-way mail relationship and will score messages more favorably. The result is that the [SPAM?] warning usually goes away on its own within a few days to weeks. This works especially well for e-mail newsletters and other 1-way correspondence.

- Reply to the Sender. When you reply to the sender, PerfectMail assumes that you are giving the sender implicit permission to continue sending you e-mail. This behavior is in line with e-mail Best Practices, as users are strongly encouraged to never reply to Spammers or opt out of Spam mail. It usually takes just one reply to cause PerfectMail to drop the [SPAM?] warning. (Note: You must reply from your original e-mail account, not an e-mail relay account. If your mail, once it is filtered, is relayed to a new e-mail address then PerfectMail will not handle the return message.)
- White-List the Sender. The last, and least desirable, alternative is to find the sending server's e-mail address and add it to PerfectMail's white list. This will cause PerfectMail to automatically accept everything (except Viruses and unwanted attachments) from that server. This step can only be performed by the PerfectMail administrator.

20.10 SPF Rejects

Message Example:

```
550-5.1.1 SPF Block: YOUR DNS says [192.168.1.13] can't send mail(ID:115I924U002784))
```

This sort of reject message occurs when a sender is blocked because of an SPF failure. Sender Policy Framework (SPF) is a great method for verifying the authenticity of e-mail. E-mail is very prone to spammers spoofing other peoples e-mail addresses. When an e-mail is crafted, you can say you are anyone you wish! Spammers take advantage of this to give themselves more credibility and deflect bounce messages to other people.

The best way to block this sort of thing is using Sender Policy Framework (SPF). SPF is implemented as a DNS entry for your domain. It specifies what hosts are valid for sending mail for your domain. Any other host should be considered a hoax.

Many e-mail hosts and even anti-spam filters are not checking SPF records, so there will always be a number of false messages being delivered; but this is the best method available to us at this time.

Some domains are having problems with their SPF records. We've seen instances where domains are not fully specifying all the machines that send e-mail for that domain.

If you are receiving these errors chances are the computer you sent the message from is not registered in the SPF record for your domain.

This sometimes happens when people send e-mail from their "Home Computer" using their "Work E-mail Address". The e-mail address you used is fine; but the "Work" domain doesn't accept your ISP's IP number (Bell, Sympatico, Rogers, Telus, etc.) as a valid relay host for their domain. If this is the case, make sure you configure your "Home Computer" to use an appropriate e-mail address. If you want people to reply to your "Work E-mail Address", then use this as the "Reply-To" in your e-mail setup.

E-mail may also get blocked when using e-mail relay sites, such as Yahoo Groups. This occurs when the relay site forwards your e-mail using your original e-mail address as the sender address. If your SPF record does not record the relay site as a valid source of e-mail for your domain, your messages will likely be blocked. This situation is best fixed at the recipient site. Add whitelist entries for relay-sites you want to accept mail from.

In general: These issues lie with the sender and their domain administrators; but life is not always that simple. If this is presenting problems you can do the following:

- Contact the sender and tell them there is a problem with their SPF record.
- White list their IP number or Domain.
- Tell the support staff at PerfectMail. We maintain a list of common relay domains that are not SPF checked.

- Or if this is a big problem, turn off SPF filtering in the Global Settings page.

You can get more information on crafting an SPF Record by going to http://www.openspf.org/. On this page there is a section called "Deploying SPF", with a web form for crafting an SPF record (currently set to example.com). Use this to craft an SPF record for your domain.

20.11 E-mail Backscatter

Backscatter is incorrect automated rejection (or bounce) messages sent by mail servers, usually resulting from incoming spam. Such messages are viewed by the recipients as a form of spam, since the recipient is (by definition) not the originator of the e-mail being rejected.

Backscatter usually occurs because worms and spam messages forge their sender address (often with legitimate e-mail addresses). Mail servers configured to send Non Delivery Reports (NDRs) will incorrectly bounce the message back to the forged sender address.

Mail servers that generate email backscatter can end up being listed on various DNS Black Lists, and be in violation of the Terms of Service of some Internet Server Providers.

PerfectMail does not make use of Non Delivery Reports (NDRs), rather it uses SMTP Rejection Notices. These rejection notices are exchanged during the SMTP mail exchange; when e-mail is being exchanged between mail servers. PerfectMail is able to give notification during the e-mail exchange because it is a Live Filtering Solution. PerfectMail analyzes, filters and responds to e-mail in real time, during the message exchange. This guarantees that PerfectMail sends a rejection notification and that the sending server received it; which is implicitly the correct server to send the notification to. By definition, such messages are not Backscatter.

20.12 Semi-Colon Delimiters: E-mail Rejected with 553 Error

This error often occurs when custom scripts are created to send e-mail notifications, mail blasts, etc. The use of any separator character other than a comma ',' is not standards compliant. The Internet Message Format RFC 2822 requires lists of e-mail addresses to be separated by the comma ',' character. A semi-colon ';' is only allowed at the end of a group specification, not to speparate addresses.

This situation can occur when programmers use a semi-colon ';' delimiter to separate addresses in e-mail address lists when creating custom e-mail routines. The confusion can occur when programmers consistently work with and test on Microsoft mail products, or other products which allow a semi-colon ';' delimiter.

Programmers should write scripts/programs which are sandards-compliant to avoid mail delivery issues.

History

The Microsoft Mail (MSMail) product was introduced for PC networks in 1991. Microsoft Mail was a shared-file mail system using a database of shared files (via mapped network drives) as the "postoffice". The Microsoft Mail product used a semi-colon ';' to delimit address lists.

The Simple Mail Transport Protocol (SMTP) commonly used for tranferring messages via the Internet specifies the use of the comma ',' to delimit addresses, in an address list.

Microsoft has kept the use of the semi-colon ';' delimiter as a proprietary standard for messages "displayed" in their mail products. However, when sending e-mail through the Internet via SMTP Microsoft servers translate the semi-colon ';' character to a comma ',' to remain standards complient.

Summary

In short, regardless of how a message is displayed in an e-mail client, it must be transmitted using SMTP standards compliant formatting (i.e. RFC 2822). Specifically, e-mail address lists must be delimited using the comma ',' delimiter.

20.13 Google™/Gmail™/Postini™ Bounces

Google™, Gmail™ and other domains use the Postini™ anti-spam service to filter e-mail. Postini will give "doubled" return codes on e-mail errors. For example:

```
 552 552 Password protected zip file found inside of the email (state 18).
```

If you see a double return code like `552 552` the message likely was rejected by the Postini service. This rejection message has nothing to do with PerfectMail™. The e-mail is being rejected by Postini, for the stated reason.

To fix the problem either change what is being sent to meet the expectations of Postini, or contact an e-mail administrator for the recipient domain.

20.14 Rogers™/Yahoo™: 554 Message not allowed - [320]

Rogers™ and Yahoo™ services (among others) will reject e-mail messages if the message date is too far into the future; giving the error:

```
554 Message not allowed - [320]
```

. In most cases this is caused by the date on the sending PC being set incorrect. If you experience this problem check the date setting on both your mail server and PCs.

20.15 What does "may be forged" mean?

PerfectMail's *Mail Transport Agent* does a reverse hostname lookup of the IP address of the connecting client, and a lookup of the IP addresses associated with that hostname. If the client IP address does not appear in that list then the "may be forged" tag is added.

20.16 Can not read winmail.dat error

If you are receiving errors from your mail client saying *can not read winmail.dat* or a similar error message, and you are not using a Microsoft e-mail client, you have a problem with the Outlook settings of the *person who sent you that e-mail*.

winmail.dat is a proprietary Microsoft method of encrypting mail, generally only understood by Microsoft programs. Non-Microsoft mail clients often can not read the *winmail.dat attachment*. This is a very common problem in e-mail.

This situation occurs when an Outlook mail client is configured to send mail formatted using *rich text* rather than *HTML*. The sending mail client needs to be configured to use *HTML* markup.

Below are instructions for disabling *winmail.dat* transmission in Outlook. Note, these tasks need to be performed on the *sender's* mail client.

20.16.1 Disable winmail.dat in Microsoft Outlook

1. Select *Tools*, then *Options*... from the menu
2. Go to the *Mail Format* tab.
3. Under *Compose in this message format*, make sure either *HTML* or *Plain Text* is selected.
4. Click *Internet Format*.
5. Make sure either Convert to Plain Text format or *Convert to HTML* format is selected under When sending *Outlook Rich Text messages to Internet recipients*.
6. Click OK.
7. Click OK again.

20.17 Excel Spreadsheet False Virus Report

We have seen cases where anti-virus signatures will sometimes trigger false positives on Microsoft Excel Spreadsheets. For example,

```
Virus Detected: BC.Exploit.CVE_2012_1847
```

If this is happening send our Support Team a message and we will fix the problem as soon as possible. False positives like this are quickly identified by our anti-virus provider (ClamVA) and an update will be pushed to you ASAP.

20.18 DHCP Issues

If the network interface is configured for DHCP and a DHCP server is not available the network interface *will not start*! Check to make sure the network interface is configured correctly. You may need to log in to the system console with userid: **root** and password: **admin** to reconfigure an interface that will not start.

20.19 Server Has A DHCP Lease, But Should Be Static

If your server has a DHCP lease, but you have configured it with a static IP address, you likely have a duplicate IP on your network. Try to ping the IP address you were expecting. If it is on the network then you need to resolve the IP address conflict.

20.20 "This Connection is Untrusted" Warnings

Accessing PerfectMail using secure HTTP (i.e. URLs starting with *https://*) and *Self-signed certificates* will result in warning messages from most modern web browsers, such as *Firefox* and *Internet Explorer*. You may receive a message saying *There is a problem with this website's security certificate* or *This Connection is Untrusted*, because the certificate is self-signed.

If possible, *Add an exception* for the self-signed certificate and *continue to the website*. These warning messages may continue to be presented by your web browser until you replace your self-signed certificate with a registered certificate. This is not necessary. If needed, certificates can be applied to your PerfectMail server under the Server Admin menu on the Administrator's web interface.

21 Server Maintenance

21.1 Increasing Hardware Resources

If you need to increase the hardware resources, simply shutdown the PerfectMail server and increase them. PerfectMail will automatically identify and make use of newly added CPU's, Memory and Storage devices. This works for both physical and virtual environments.

Added *hard drives* are automatically appendended to the PerfectMail data volume and formatted to increase the disk storage available to PerfectMail. All you have to do is install the drive (physical or virtual) and boot PerfectMail.

21.2 Migrating to a New PerfectMail Server

To migrate your settings from an existing PerfectMail™ server to a new one use the following procedure:

1. You can get an install ISO from our website: http://perfectmail.com on the Downloads page; install the new PerfectMail™ server from this ISO.
2. On your old server go to the "Server Admin => Backup" page and create a configuration backup file. Click on the backup description to download the backup to your PC.
3. On the new server go to the "Server Admin => Backup" page and upload the backup file.
4. Click on "Restore Server" to duplicate all the settings of the old server, including network settings; or click "Restore Settings" to restore everything BUT the server's network settings.

Note: the license is not copied. Each new server install needs to have a unique activation code applied to it. During the install the server should have acquired a demo license. When you're ready, we'll get you a new activation code.

This process only copies over the server settings. Future enhancments to PerfectMail will allow you to copy over your e-mail history as well.

22 Reference

22.1 Resetting Network Settings

If it is not possible to reconfigure the network settings using the web user interface you can reset the settings via the server console. You must login on the console in order to perform this task. Login to the console with the following credentials:

Userid: netconfig
Password: *(The password for your "root" account.)*

You can now reset the basic network settings for this server. Please take care and ensure these settings are functional:

- Host Name - Must be a fully qualified host name (E.g myhost.mydomain.com). This should be a name that is resolvable using DNS. Remember, this server will be visible to the Internet; giving it an unresolvable host name may cause other mail servers to reject your e-mail.
- IP Address - The static IP address of this server using standard 4-octet notation: (E.g. 192.168.1.100)
- Netmask - The netmask of this server using standard 4-octet notation: (E.g. 255.255.255.0)
- Default Gateway - The default gateway for this network segment.
- Primary DNS Server - Remember, DNS resolution must work for your PerfectMail server to function. PerfectMail will not accept e-mail from unresolvable domains!

22.2 A Definition of Spam

The word *spam* as applied to e-mail means Unsolicited Bulk Email ("UBE").

Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Examples include: first contact inquiries, job inquiries, sales inquiries, etc.

Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content. Examples include: subscriber newsletters, customer communications, discussion lists, etc.

The technical definition states a message is spam only if it is both *unsolicited* and *bulk*.

Spam is an issue about consent, not content. Whether the UBE message is an advert, a scam, porn, a begging letter or an offer of a free lunch, the content is irrelevant; if the message was sent unsolicited and in bulk then the message is spam.

Spam is not a subset of UBE. It is not "UBE that is also a scam or that does not contain an unsubscribe link". All email sent unsolicited and in bulk is spam.

This distinction is important because legislators spend inordinate amounts of time attempting to regulate the content of spam messages, and in doing so come up against free speech issues.

Important facts relating to this definition:

1. The sending of *Unsolicited Bulk Email* ("UBE") is banned by all legitimate Internet service providers worldwide.
2. Real-time Block Lists are used by hundreds of millions of Internet users to reject emails identified as spam. These lists are based on the internationally accepted definition of spam as *unsolicited bulk email*. Therefore

anyone sending UBE on the Internet, regardless of whether the content is commercial or not, illegal or not, needs to be fully aware that they will lose their Internet access if they send UBE and they will be placed on the Real-time Block Lists.

3. All a spammer has to do is **GET YOUR PERMISSION** and they can spam you with impunity.

The last point above is currently a huge issue. All the spammers have to do is to get your e-mail address and permission, then they can spam you with impunity. At PerfectMail™ we call these spammers "industrial spammers" or "spamvertizers". They are by far the biggest problem we are now encountering.

While they technically gain impunity by skirting the law, at PerfectMail™ we expand our definition of spam to include messages where the sender attempts to hide who they are or where they are coming from.

22.3 Microsoft Exchange™

22.3.1 Configuring a SmartHost for Microsoft Exchange™

22.3.1.1 Microsoft Exchange™ 2003

In Exchange 2003, it's possible to configure a smart host on the Default SMTP Virtual Server, but if you do it this way you can only set a single smart host. The preferred method, therefore, is to use an SMTP Connector for your outgoing emails which does allow multiple smart hosts to be specified.

Following are the steps to have Microsoft Exchange 2003™ System deliver outbound mail via a Smart Host:

1. Open up the Microsoft Exchange System Manager (Start > Programs > Microsoft Exchange > System Manager);
2. Expand "Administrative Group", <Your Groupname>, you may have more than one, "Servers", <SERVER NAME>, "Protocols", "SMTP", "Default SMTP Virtual Server";
3. Right-click on "Default SMTP Virtual Server" and select Properties;
4. Click on "Delivery" tab and select the "Advanced" button;
5. Enter the Address of the hosting PM for the "Smart Host" field. You can specify the IP Address e.g.. [192.168.3.44] (using the square brackets) or use a FQDN "yourhost.yourdomain.com" (without the quotes);
6. Click on "Apply", then "OK" for all cascading windows.

These changes should take place on the fly, there is no need to restart the Exchange services.

Note that the above procedures assumes that you have a straight-forward Exchange system in place with pre-defined Exchange Routing Groups in place and that there is only one Exchange system within your organization. If you have an Exchange environment consisting of a Front-End system and a Back-End system, then the above needs to be applied on the Back-End system only.

Alternatively, you may decide to use a connector which routes email, rather than an SMTP virtual server:

1. Open up the Microsoft Exchange System Manager (Start > Programs > Microsoft Exchange > System Manager);
2. Right-click on {Your Exchange Server} and select Properties;
3. Make sure the checkbox Display routing groups is checked;
4. Right Click "First Organization";
5. Locate the folder: Administrative Groups/{Your_Administrative_Group}/Routing Groups/{Your_Routing_Group}/Connectors;
6. Right-click Connectors, select New, and then click SMTP Connector;
7. Fill in the Name field;

8. In the Smart host box, type the hostname or IP address (wrapped in square brackets [ ]) of the smart host server and select the local bridgehead (usually your mail server);
9. Select the Address Space tab, typical settings are "SMTP" and select (*).

If the above procedures do not work for you and you have restarted the Exchange services (or rebooted the Exchange Server) then there is a possibility that you may have a custom Routing group defined with a custom SMTP connector for all SMTP Address Spaces and SMTP connector configurations within the Routing Group section take precedence over the default virtual SMTP protocol configurations within the Protocols section.

22.3.1.2 Microsoft Exchange™ 2007/2010

For Exchange 2007/2010 configure a default relay host (smarhost) by creating a Send Connector. With Exchange 2007/2010, Microsoft has separated the mail server roles. The Hub Transport role is responsible for sending and receiving external email. In a single Exchange server environment, the same server will perform all roles.

1. Open the Exchange Management Console;
2. Expand the Organization Configuration (click on the "+" next to Organization Configuration);
3. Select Hub Transport, then the Send Connectors tab;
4. Right-click on the existing Send Connector;
5. Select Properties, then the Network tab;
6. Select "Route mail through the following smart hosts:" and click Add;
7. Enter the internal IP address of your smarthost relay server.
8. Click OK.

Once you click OK the changes will take effect immediately.

Enabling SMTP Recipient Filtering for Microsoft Exchange™

Following are the steps to enable **recipient filtering** to allow PerfectMail™ to validate e-mail users for Microsoft Exchange™.

When recipient filtering functionality is enabled, it filters all messages that come through all Receive connectors on that computer. By default, recipient filtering is enabled on the computer that has the Edge Transport server role installed for inbound messages that come from the Internet but aren't authenticated. These messages are handled as external messages. If this feature is turned off **all e-mail addresses will be accepted** by both Exchange and PerfectMail™.

Please ensure you have the appropriate permissions to perform this task.

22.3.1.3 Microsoft Exchange 2003™

Please enable **recipient filtering** by doing the following:

1. Open Up Exchange System Manager.
2. Expand "Global Settings".
3. Right-click on "Message Delivery" and select "Properties".
4. Select the "Recipient Filtering" tab.
5. Check "Filter recipients who are not in the Directory" and click on "Apply".
6. A big warning message will come up regarding manually enabling filtering on specific SMTP virtual server. Click "OK".
7. Click "OK" to close "Message Delivery Properties".
8. You should now be back at the Exchange System Manager screen at this point. Expand "Administrative

Group".
9. Expand the Information Store group. (There may be more than one within your organization.)
10. Expand "Servers", then <your server name>, then "Protocols".
11. Highlight "SMTP" and you should see the SMTP server configuration. (Default name is "Default SMTP Virtual Server".)
12. Right click "Default SMTP Virtual Server" and select "Properties".
13. The "General" tab will be open. Click on "Advanced" beside the "IP Address field".
14. An advanced window will pop up. Leave the default selection as is.
15. Click "Edit" and that will bring up the Identification window.
16. Check to enable "Apply Recipient Filter" and click "OK" and then "OK" again.
17. Click on "Apply", then "OK".
18. Repeat steps 12-17 for each SMTP protocol.
19. Repeat steps 9-17 for multiple store groups (if applicable).
20. There is no need to restart any Exchange services. Changes may take a few minutes to take effect as it may be replicated.

22.3.1.4 Microsoft Exchange 2007/2010™

With Exchange 2007/2010, Microsoft has separated the mail server roles. The Edge Transport role is responsible for recipient filtering. In a single Exchange server environment, the same server will perform all roles.

Use the Exchange Management Console to enable or disable recipient filtering:

1. Open the Exchange Management Console on the Edge Transport server.
2. In the console tree, click Edge Transport.
3. In the work pane, click the Anti-spam tab, and then select Recipient Filtering.
4. In the action pane, click Enable or Disable as appropriate.

Use the Shell to enable or disable recipient filtering:

1. Set-RecipientFilterConfig -Enabled $true

For detailed syntax and parameter information, see Set-RecipientFilterConfig.

22.4 ClamAV Anti-Virus

PerfectMail™ is built with the Clam Anti-Virus engine. ClamAV is a professional grade anti-virus engine that offers a number of benefits:

- ClamAV is small, fast and efficient.
- ClamAV checks for virus signature updates every ten minutes.
- Scanning at the gateway keeps viruses off your mail server.
- ClamAV catches more than Viruses. The ClamAV engine has been leveraged to block phishing and social engineering attacks, including bank scams and other fraud related attacks.

ClamAV has been tightly integrated into PerfectMail™. The result is an anti-virus scanning engine that is very fast and efficient.

We recommend three levels of virus scanning for any organization:

1. At the gateway. (Using PerfectMail™ of course!)
2. At the server.

3. At the desktop.

22.5 Enabling Mail Headers in PerfectMail

To use Distributed Filtering you must enable specific mail headers in PerfectMail. Using your web browser, log into the PerfectMail administrative interface and go to the "Filtering > Filter Settings" page. At the bottom of this page you will find a section on "Mail Headers". Ensure the "Spam flag header" and "Spam level header" settings are checked.

22.6 Enabling Mail Header Filtering in Your E-mail Client

You can create filter rules on your local e-mail client (e.g. Microsoft Outlook™) to automatically file messages in your "Spam" or "Junk" folder. For sites that are particularly concerned about loosing e-mail, or even for specific users, you can have PerfectMail not reject any e-mail and use these filtering rules to filter messages on your local e-mail client.

This section describes how to implement Distributed Filtering for several popular e-mail clients. The steps for other e-mail clients are likely very similar to those presented here.

22.6.1 Microsoft Outlook Express™ Filters

1. Go to Tools->Message Rules->Mail...
2. Check 'Where the Message Body contains specific words'
3. Select 'Where the Message Body contains specific words '.
4. Click on 'contains specific words'.
5. Type in: X-Spam-Flag: Yes (one space between the : and the Yes)
6. Click 'Add'.
7. Click 'Ok'.
8. Select 'Move it to the specified folder'.
9. Click on 'specified'.
10. Highlight an existing folder, or create a new one.
11. Click 'Ok'.
12. Give the rule a name. (The default is New Mail Rule #1.)
13. Click 'Apply Now'. (You may or may not want to Apply Rule Now)
14. Click 'OK'.

22.6.2 Microsoft Outlook™ Filters

1. Go to Tools->Rules Wizard...
2. Click 'New...' (On the top right)
3. Choose 'Check messages when they arrive'
4. Click 'Next'.
5. Check 'With specific words in the message header'.
6. Click on 'specific words'.
7. Type in: X-Spam-Flag: Yes (one space between the : and the Yes)
8. Click 'Ok'.
9. Click 'Next'.
10. Check 'Move it to the specified folder'.
11. Click on 'specified'.
12. Highlight an existing folder, or create a new one.
13. Click 'Ok'.
14. Click 'Next'.
15. Click 'Next'. (Again, unless you want to add exceptions.)

16. Give the rule a name. (The default is what you typed for "specific words", above.)
17. Check 'Turn on this rule'. (You may or may not want to check 'Run this rule on my Inbox now'.)
18. Click 'Finish'.

22.6.3 Microsoft Outlook 2002™ Filters

Microsoft Outlook 2002™ does not have the ability to filter spam itself, but it has filtering "rules" that we can use. The Rules Wizard will only appear in the Tools menu when the Inbox is selected, so choose the Inbox before you try to add a filter.

1. Select "Inbox" in the Folder List.
2. Click "Tools" and select "Rules Wizard".
3. Click "New" to create a new rule.
4. Check "Start from a blank rule" and select "Check messages when they arrive". Click "Next".
5. Check "with specific words in the message header".
6. In the rule description, click "specific words".
7. Under Specify a word or phrase to search for in the message header, enter "X-Spam-Flag: YES" to put spam into your "Spam" folder". Click "Add", then "OK", and finally "Next".
8. Under "What do you want to do with the message?", check "move it to the specified folder".
9. In the rule description, click "specified".
10. Under Choose a folder, click "New".
11. Enter "Spam" as the name and click "OK"
12. Select "Spam" under Personal Folders (click the plus sign to open Personal Folders if necessary) and click "OK", then click "Next" twice.
13. Click "Finish".

22.6.4 Microsoft Outlook 2003™ Filters

Microsoft Outlook 2003™ includes spam filtering. Outlook will filter messages based on its own concept of spam, but you can also have it put spam messages identified by PerfectMail in your "Junk" folder.

1. Select "Inbox" in the Folder List.
2. Select "Tools" and then "Rules and Alerts".
3. View the E-mail Rules tab.
4. Click "New Rule..."
5. Check "Start from a blank rule" and select "Check messages when they arrive". Click "Next".
6. Check "with specific words in the message header".
7. In the rule description, click "specific words".
8. Under Specify a word or phrase to search for in the message header, enter X-Spam-Flag: YES to put spam in your "Junk" folder. Click "Add", then "OK", and finally "Next".
9. Under "What do you want to do with the message?", check "move it to the specified folder".
10. In the rule description, click "specified".
11. Under Choose a folder, select "Junk E-mail" and click "OK".
12. Click "Finish".

22.6.5 Macintosh OS X™ Filters

Macintosh OS X™'s built-in Mail program can create filters based on custom headers.

1. In the menu bar, click 'Mailbox' then 'New Mailbox' and create the mailbox you want the Spam to end up in.
2. In the menu bar, click 'Mail' then 'Preferences...'
3. Click 'Rules' then 'Create Rule'.

4. Add a description of the rule, then click the 'From' Criteria, then click 'Expert...'
5. In the Header: field enter 'X-Spam-Flag', click 'Add Header' and 'OK'
6. Now click 'From' and select 'X-Spam-Flag'. Select 'Contains' in the next box and enter 'Yes' in the third Criteria box.
7. In the Action section, check 'Transfer to mailbox' and select the desired mailbox. Click 'OK'.
8. Adjust the rule priorities if you want, and dismiss the Mail Preferences dialog box.
9. The next time you check your mail, check to see if any messages were automatically filtered into your Spam mailbox!

22.6.6 Outlook Express™ for Macintosh™

The instructions are the same as for Outlook Express 4.5 and 5.x for Mac, but the menu item under Tools is called "Mail Rules" in version 4.5 and "Rules" in version 5.x. Also, there's no choice between POP/IMAP. Note: if you are sending messages found by this rule to a special mail folder, you must already have created the destination folder before you create the rule.

1. From the menu bar, choose Tools; then "Rules" or "Mail Rules" depending on your Outlook Express Version (5.x and 4.5 respectively.
2. Select POP, and then hit "new" for a new rule.
3. Under the section marked "If", choose "specific header" and then type or paste in the name of the header, which is "X-Spam-Flag".
4. Under "Contains:" type in Yes.
5. In the section marked "Then", specify an action -- move to a new folder, change its status or color, as you see fit. Note that we do not recommend simply deleting messages found by this rule.
6. The Enabled box needs to be checked in order for this rule to be active - it will be checked by default.

22.6.7 Netscape™ Filtering

Netscape 6.2.1 does not allow you to create custom filters, so users of this version are unable to take advantage of the special headers used in their mail client software at this time.

Netscape 4.7.8 allows you to create a custom filter. You can supply the special x-header information to Netscape 4.7.8 by doing the following:

1. In the pull-down bar at the top of your Netscape 4.78 window, go to "Edit: Message Filters". A new window will open.
2. Click "New". Click "Advanced". A new window will open.
3. Enter "X-Spam-Flag", click "Add", and click "OK". The latest new window will close.
4. In the pull-down list, select "X-Spam-Flag".
5. In the "contains" box, enter "X-Spam-Flag: Yes".
6. In the "Perform this action" pull-down list, select "move to folder".
7. Click "new folder" and create a Spam folder. It should then be selected in the pulldown list of your folders.
8. Click OK.
9. The next time you check your mail, check to see if any messages were automatically filtered into your Spam folder!

22.6.8 Evolution™ Filters

Ximian Evolution™ is an email client for Linux similar to Microsoft Outlook™. It is installed by many Linux™ distributions including Red Hat™, Fedora™, and SuSE Linux™. Evolution™ has the ability to filter on an arbitrary header as well as on the send and receive addresses.

1. Click "Inbox" to display the Inbox.
2. Click "Edit" and select "Message Filters". (Sometimes "Filters is located under "Tools".)
3. In the Filters window, click "Add".
4. Enter a name for the filter under "Rule name".
5. Under "Find items that meet the following conditions", choose "Specific header" in the leftmost button menu; in the field to the right of "Specific header", enter "X-Spam-Flag"; change the button beside this to read "is"; and enter "YES" in the last field.
6. Under "Then", choose "Move to Folder".
7. Click "click here to select a folder".
8. Click "New", enter SPAM as the folder name, select "Local Folders", and then click "OK" for each window until you get back to the main window..

23 PerfectMail™ License Agreement

PerfectMail™ License Terms and Conditions

PerfectMail™ IS WILLING TO LICENSE THE SOFTWARE YOU ARE ABOUT TO USE ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. THIS IS A BINDING AGREEMENT BETWEEN YOU (THE "CUSTOMER") AND PerfectMail™. YOU MUST AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT IN ORDER TO USE THE SOFTWARE OR SUBSCRIBE (EITHER AS A PURCHASER OR FOR A TRIAL PERIOD) TO PerfectMail™ SERVICES. BY PROCEEDING TO RUN THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "I AGREE" LINK AT THE BOTTOM OF THE AGREEMENT OR BY SIMPLY USING THE PRODUCT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, RETURN THE PRODUCT TO THE PLACE OF PURCHASE.

1. DEFINITIONS

In this Agreement,

1.1. *Company* means PerfectMail™, the developer of Product. A legal entity officially known as 789852 Ontario Inc. incorporated in the Province of Ontario, Canada.

1.2. *Software* means the object code version of the computer software licensed by Customer under this Agreement.

1.3. *Documentation* means such manuals, documentation and any other supporting materials relating to the Licensed Software as are currently maintained by PerfectMail™ and generally provided to its licensee.

1.4. *Product(s)* means hardware, Software, documentation, accessories, supplies, parts and upgrades that are determined by PerfectMail™ to be available from PerfectMail™ upon receipt of Customer's order.

1.5. *Reseller* means a dealer Licensed by PerfectMail™ to sell its products.

1.6. *Customer* Any licensee of PerfectMail™ products including, but not limited to, PerfectMail™. This term will also be used for organizations who wish to or are currently evaluating Product regardless of their ultimate decision to acquire a License or purchase Product.

1.7. *Access* Any direct or indirect computer/electronic access to any physical appliance, virtual appliance, customer server or managed service running Product. This includes, but is not limited to secure command line, web, graphics user interface, e-mail or other direct or indirect access.

1.8. *Customer Agreement* means the agreement between the Customer and the Reseller and/or PerfectMail™ setting out the type of License and License Fee for the products and/or services provided.

1.9. *License* means the Software and Support License or Evaluation License granted for the appropriate number of Terminals, License Fee and Term of Validity as set out in any accompanying Customer Agreement

1.10. *License Fee* means the fee or fees designated by PerfectMail™ or the Reseller for Software and Support. Different License Fees apply depending on the type of License, the duration of the License, and the nature of the support.

1.11. *Term of Validity* means the period set out in the accompanying Customer Agreement throughout which Customer may use the software either on the basis of an Evaluation License or a Software and Support License.

2. LICENSE TERMS

2.1. Software is owned and copyrighted by PerfectMail™ and/or by third party suppliers. Customer's Software and Support License confers no title or ownership and is not a sale of any rights in the Software. Third party suppliers shall have the rights to protect its own proprietary rights to the Software in the event of any infringement.

2.2. Unless otherwise permitted by PerfectMail™, Customer may only make copies of the Software for archival purposes or when copying is an essential step in the authorized use of the Software on a backup device, provided that copies are used in no other manner and provided that the use on the backup device is discontinued when the original or replacement device becomes operable.

2.3. Customer may not use more appliances than stipulated in the License, nor may the software be used if it is not within the Term of Validity of the most recent License or Support Agreement with the Customer.

2.4. Customer will not modify, disassemble or decompile the Software without PerfectMail's prior written consent. Where Customer has other rights under statute, Customer will provide PerfectMail™ with reasonably detailed information regarding any intended disassembly or decompilation. Customer will not decrypt the Software unless necessary for legitimate use of the Software. In addition Customer will take all reasonable steps to ensure that users of PerfectMail's software in Customer's possession do none of the aforementioned.

2.5. Customer will not remove any product identification, copyright notices, or other notices or proprietary restrictions from the Software unless this option is provided as a configuration option by the Software.

2.6. Customer will not disclose results of any benchmark tests of the Software to any third party without PerfectMail's prior written approval;

2.7. Customer will not install or use demo, demonstration or evaluation licenses for any purpose other than for evaluation purposes;

2.8. Customer will not sell, transfer, lease or otherwise assign free licenses to any other party.

2.9. If Customer does not renew a license agreement with PerfectMail™ by the termination date, customer agrees that the Product will no longer be supported, that updates will not be provided, that signature files will not be updated and that customer will not be entitled to bug fixes, defect repairs, feature enhancements or other benefits.

2.10. PerfectMail™ may terminate Customer's License upon notice for failure to comply with any applicable License terms.

3. LICENSE GRANT

3.1. Subject to timely payment of the products and/or License Fees and the terms and conditions of this Agreement, PerfectMail™ grants Customer a non-exclusive and non-transferable license to use the Software embedded within our products during the Term of Validity of the License in conformance with:

3.1.1. The terms set forth herein;

3.1.2. Use restrictions and authorizations for the Software specified in the Customer Agreement;

3.2. Some of the Software Programs included in PerfectMail's software are distributed under the terms of agreements with Third Parties ("Third Party Agreements") that may expand or limit Customer's rights to use certain Software Programs as set forth in Section 2. Certain Software Programs may be licensed (or sub-licensed) to Customer under the GNU General Public License and other similar open source license agreements ("OSLAs") which, among other rights, permit Customer to copy, modify and redistribute certain Software Programs, or portions thereof, and have access to the source code of certain Software Programs, or portions thereof. In addition, certain Software Programs, or portions thereof, may be licensed (or sub-licensed) to Customer under terms stricter than those set forth in Section 2.

3.3. Unless the Customer is a PerfectMail™ authorized reseller, Customer may not sub-license the Software unless otherwise agreed to by PerfectMail™ in writing.

4. LIMITED WARRANTY

4.1. PerfectMail™ warrants that the Software will perform substantially in accordance with administrator manual or readme file of the Licensed Product during the Term of Validity of the most recent License.

4.2. PerfectMail's and its licensor's' entire liability and Customer's exclusive remedy shall be, at PerfectMail's option, either:

4.2.1. Return the prorated License Fees for the current period, or

4.2.2. Replacement of Software that does not meet PerfectMail's Limited Warranty. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplications.

4.3. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PerfectMail™ AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE, WITH REGARD TO THE SOFTWARE AND THE ACCOMPANYING ITEMS.

5. FEES AND TAXES

5.1. All fees payable to PerfectMail™ are due at the commencement of the License Period. Customer agrees to pay any sales, value-added or similar taxes imposed by applicable law that PerfectMail™ must pay based on the services that Customer ordered.

6. INDEMNIFICATION

6.1. PerfectMail™ shall defend, at its sole discretion, or settle any action, claim or demand brought against Customer on the basis of infringement of any copyright, trademark, trade secret or patent (the "Intellectual property Rights") by the Software or use thereof. PerfectMail™ shall pay any final judgment entered into against Customer in such action provided that PerfectMail™ has the sole control of the defense and/or settlement and Customer promptly notifies in writing of such claim and provides all information known to the Customer relating thereto, and Customer cooperates with PerfectMail™ in the defense and/or settlement. Should the Software become or in PerfectMail's opinion may become the subject of infringement of any Intellectual Property Rights, PerfectMail™ may, at its expense do one of the following:

6.1.1. Replace the Software or affected part with non-infringing programs;

6.1.2. Modify the Software or affected part to make it non-infringing;

6.1.3. Procure for Customer the right to use the Software; or

6.1.4. If none of the alternatives are commercially reasonable, PerfectMail™ may refund the prorated License Fees received from Customer for the current Term of Validity.

6.2. PerfectMail™ shall have no indemnification obligation to the extent a claim is based upon:

6.2.1. The combination, operation or use of the Software with any products or services not provided by PerfectMail™; or

6.2.2. The use of the Software in a manner not authorized by this Agreement.

6.3. THIS SECTION PROVIDES THE ENTIRE OBLIGATION OF PerfectMail™ AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO THE INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

7. Indemnification by Customer

7.1. Customer agrees that it shall fully indemnify and completely save harmless PerfectMail™ and any of its directors, officers, employees, agents, representatives of and from any and all liabilities, claims, expenses, damages including reasonable legal fees and disbursements arising out of any claims or suits for damage or injury to person in connection with, directly or indirectly, in whole or in part, (i) any negligent act or omission of the Customer's employees, agents, contractors, directors, officers or any person for whom it has a legal responsibility or (ii) the failure of Customer to comply with any municipal, provincial or federal law or (iii) any act or omission which is, or can be determined to be, a breach of any term or condition of this Agreement.

8. NON-DISCLOSURE OF PERFECTMAIL INFORMATION

8.1. The Software and other proprietary information provided by PerfectMail™ hereunder contain and constitute trade secrets, information and data proprietary to copyright by PerfectMail™. Customer shall use a reasonable degree of care to protect the confidentiality of the Software and shall not cause or permit such confidential information or data to be disclosed to third parties or duplicated except as permitted in this Agreement. Customer acknowledges and agrees that unauthorized disclosure, use or copying of the Software may cause PerfectMail™ irreparable injury. Accordingly, in the event of any unauthorized disclosure, use or copying of the Software, Customer agrees that PerfectMail™ shall have the right to seek injunctive or other equitable relief. Each party will not disclose or use any business and/or technical information of the other designated in writing or orally (and promptly confirmed in writing) as *Confidential* ("Confidential Information") without the prior written consent of the other party. Such restrictions do not extend to any item of information which:

8.1.1. Is or becomes available in the public domain without the fault of the receiving party;

8.1.2. Is disclosed or made available to the receiving party by a third party without restriction and without breach of any relationship of confidentiality;

8.1.3. Is independently developed by the receiving party without access to the disclosing party's Confidential Information,

8.1.4. Is known to the recipient at the time of disclosure, or

8.1.5. Is produced in compliance with applicable law or court order, provided that the disclosing party is given reasonable notice of such law or order and an opportunity to attempt to preclude or limit such production.

9. NON-DISCLOSURE OF CUSTOMER INFORMATION

PerfectMail™ acknowledges that the information retained on Product or otherwise received or generated, directly or indirectly, while working with Customer is highly confidential in nature and must be treated with the utmost discretion. As such, the following conditions are reasonable. Therefore, PerfectMail™ hereby agrees as follows:

9.1. PerfectMail™ will ensure that all officers, employees, contractors or associates who have direct or indirect access to Customer Product, data or information will be covered under individual Non-Disclosure Agreements.

9.2. PerfectMail™ will access Customer Product only while providing support and/or updating Product. Company will seek from Customer prior consent for any access outside of support and update.

9.3. Customer shall have the option to provide Company with blanket consent or consent on an incident by incident basis. Customer shall retain the option of changing consent at any time. PerfectMail™ must be provided notice before changes to consent take effect.

9.4. PerfectMail™, its officers, employees, contractors or associates will hold any information viewed while working on Customer Product in the strictest confidence. This includes, but is not limited to Product configuration information, the contents of any log or archive information viewed while working on Product or any other information that could be reasonably deemed to not be in the Public Domain.

9.5. For back up and recovery purposes or to improve Customer experience with Product, PerfectMail™ may retain copies of Customer Product configuration information on PerfectMail's servers.

9.6. PerfectMail™ will not duplicate, transfer, retain or otherwise copy Customer Product e-mail archive or e-mail contents from Product without prior consent of Customer.

9.7. PerfectMail™ normally receives aggregate performance data from Customer Product as part of our Product health and performance monitoring capabilities. No personal information is included in this performance data.

9.8. To ensure compliance with purchased license limits or to ensure accurate billing, PerfectMail™ may, from time to time, review reported resources from Product.

9.9. PerfectMail™ will not provide confidential Customer information to third parties without prior written consent from Customer, unless compelled by law.

9.10. PerfectMail™ will not use Customer information for any purpose other than as indicated in this agreement without first seeking Customer's prior written consent.

9.11. At the end of any contracts or agreements, and when Customer's obligations to PerfectMail™ are fully discharged, Customer may request that PerfectMail™ destroy all technical records relating to the support of Product. Alternatively, PerfectMail™ may destroy all Customer data at the end of contract or agreement covering such data. PerfectMail™ is under no obligation to maintain backups or archives of Customer configuration information.

9.12. PerfectMail™ is governed by and will comply with all Privacy and Confidentiality laws for Canada and the Province of Ontario.

10. DATA COLLECTION AND NOTIFICATION

10.1. PerfectMail™ may collect statistical and status information from your server for support and analysis purposes. At no time is e-mail message content sent from the Software Product to PerfectMail™, except for any messages the Customer has reported as spam for analysis.

10.2. By default, data reporting options are enabled. It is Customer's responsibility to review the Data Disclosure document and Product Documentation for more information on data reporting, disclosure and privacy.

10.3. PerfectMail™ has provided options in the Product for the Customer to disable data collection functionality. It is the Customer's responsibility to disable any data collection or reporting functions.

10.4. PerfectMail™ maintains a list of e-mail addresses reported by the Customer for support and notification purposes. These e-mail addresses are used for sending server and product status notifications and product update messages. If Customer does not wish to receive notification messages they must contact PerfectMail™ staff and request removal from the mailing list for their PerfectMail™ server.

10.5. PerfectMail™ may from time to time, request that Customer provide PerfectMail™ with access to Product. Normally, we require access as part of its support and update obligations outlined in PerfectMail's current Support agreements. Other circumstances may also arise whereby PerfectMail™ may desire access to Product. All access is at Customer's discretion.

10.6. PerfectMail™ makes reasonable efforts to secure and keep private all Customer data including content, e-mail addresses, status and statistic information. Customer data, including e-mail addresses, will not be shared with any third party unless required by law.

11. LIMITATION OF LIABILITY

11.1. IN NO EVENT SHALL PerfectMail™ OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE EVEN IF THE COMPANY OR ANY OF ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.2. IN NO EVENT SHALL PerfectMail™ OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR PERSONAL PROFITS, BUSINESS OR PERSONAL INTERRUPTION, BUSINESS OR PERSONAL INVESTIGATION, LOSS OF BUSINESS OR PERSONAL INFORMATION, OR LOSS OF EMPLOYMENT) ARISING OUT OF THE ACCESS, DOWNLOADING, EXAMINATION, PROCESSING, LOGGING, FILTERING OR FAILURE TO FILTER ANY CONTENT (INCLUDING BUT NOT LIMITED TO E-MAIL AND WEB CONTENT) BY PerfectMail™.

11.3. Customer understands and agrees that E-mail may contain content that is offensive or illegal. Further, Customer understands and agrees that anti-spam functions may transfer content from remote sites to your PerfectMail™ server for analysis; this content may also be offensive or illegal. PerfectMail™ accepts no responsibility or liability for content from any source that may be encountered during anti-spam processes. Any action taken by Customer with respect to content accessed, downloaded, examined, logged, filtered or not filtered by PerfectMail™ is the customers total responsibility and liability.

11.4. Customer understands that PerfectMail™ may take actions in the process of analyzing e-mail from spam that may appear to processes and software that analyze network traffic to be the actions of user's e-mail addresses. PerfectMail™ takes reasonable steps to minimize such traffic, however Customer is reponsible for differentiating between PerfectMail automated anti-spam processes and the actions of other systems and users on their network. PerfectMail™ accepts no responsibility or liability for any intrepretation, misinterpretation or actions which may or not be taken based on network traffic, content analysis or logging or any other computer or business process or system.

11.5. Any action against PerfectMail™ must be brought within twelve (12) months after the cause of action arises. For purposes of this Section, "PerfectMail™" includes its directors, officers, employees, subcontractors, agents and suppliers.

12. TERM AND TERMINATION

12.1. The Software and Support License is subject to renewal at the end of the License Period. Unless renewed under an extension of the Customer Agreement, the License to use the Software will terminate.

12.2. This Agreement may be terminated if either party fails to perform any of its duties or obligations hereunder and fails to substantially cure such default within ten (10) days after written notice is given to the defaulting party. Upon an event of default, the non-defaulting party may terminate this Agreement by providing written notice of termination to the defaulting party, reserving unto the non-defaulting party all other rights and remedies it may have under this Agreement. If Customer is in default, PerfectMail™ reserves the right, in addition to all other rights and remedies it may have, to withhold further performance of its obligations under this Agreement and may repossess the Software and Documentation.

12.3. Upon termination of any license granted hereunder, Customer will promptly remove all Software from all memory locations, and destroy or return all copies of the Software and Documentation to PerfectMail™.

13. GENERAL

13.1. Customer may not assign any rights or obligations hereunder without prior written consent of PerfectMail™, which consent can be unreasonably withheld.

13.2. Customer who exports, re-exports or imports PerfectMail™ Hardware and Licensed Software, technology or technical data purchased hereunder, assumes responsibility for complying with applicable laws and regulations and for obtaining required export and import authorizations. PerfectMail™ may suspend performance if Customer is in violation of any applicable laws or regulations.

13.3. If any term or provision herein is determined to be illegal or unenforceable, the validity or enforceability of the remainder of the terms or provisions herein will remain in full force and effect.

13.4. Except as specifically provided in Section 3.1.2, these PerfectMail™ Software and Support License Terms supersede any previous communications, representations or agreements between the parties, whether oral or written, regarding transactions hereunder. Customer's additional or different terms and conditions will not apply. These PerfectMail™ Software and Support License Terms may not be changed except by an amendment signed by an authorized representative of each party.

13.5 This license does not obligate PerfectMail™ to provide support for products licensed under free or trial licenses.

14. GOVERNING LAW

14.1. This Agreement shall be governed by and interpreted in accordance with the laws of Ontario, Canada, without reference to conflict of law principles. Customer and PerfectMail™ agree to the exclusive jurisdiction of the courts located in Brampton, Ontario, Canada.

15. PARTIAL INVALIDITY.

15.1. Both parties to this Agreement hereby acknowledge that neither of them intends to violate any public policy, statutory or common laws, rules, regulations, treaties, or decisions of any government agency or executive body of any country or community or association of countries.

24 Data Collection Disclosure

Introduction
Following is a full disclosure of all data reported to PerfectMail™ from a PerfectMail™ product. PerfectMail™ is a *high touch* product giving the following benefits:

- *Statistical Reporting* gives us clear & early warning of developing spam trends.
- *Server Monitoring* ensures early notification of problems.
- *Quick & Effective* customer support.
- *Off-site Backups* provide additional peace of mind. If needed we can quickly provide assistance or build a *fully configured* replacement machine.

Automatic Server Updates
The following updates occur automatically. To disable automatic updates, update the related settings on the *Security Settings* page.

- *Anti-virus Update:* Virus update checks are performed every 10 minutes. If an update is available, it will be installed automatically.
- *Anti-spam Update:* Anti-spam update checks are performed once a day. If an update is available, it will be installed automatically.
- *Software Update:* Software updates are performed by PerfectMail™ staff, when available; and only if access is granted.

Server Support Data
The following data elements are normally reported back to PerfectMail™ for support and analysis purposes. To disable any of these reporting features update the *Server Admin=>Server Settings* page on the *Web Interface*. If support & reporting features are disabled your PerfectMail™ product will still send notification that these features are disabled. **No e-mail message content is ever sent to PerfectMail™; except for those messages the client wishes to have examined for spam content.**

- Statistical Reporting: This hourly report consists of statistical information regarding the effectiveness of the anti-spam software. E.g. number of rejects, tags, accepts, RBL's, mining attempts, spam traps, etc.
- Report Spam: The client user or administrator forwards a spam e-mail to PerfectMail™ for review. Included with the reported spam e-mail are the PerfectMail™ server name and the name of the submitting user.
- Server Monitoring: Hourly health reports allow us to see if there are any issues with the product as a whole, and databases in particular. These messages describe the state of the databases, but do not include any elements of their content. If there is an issue with a database, a notification message containing the machine name and data table name is sent to PerfectMail™ for further attention. (PerfectMail™ is able to self-fix its databases. Administrator intervention is rarely required.) Additionally, in the event of a process crash, a core file (describing what the program was doing the issue occurred) may be sent for analysis.
- False Positive Investigation: For each false positive release, a message is sent to PerfectMail™. If the client has requested *false positive investigation*, we may examine the message to determine what the problem may be. In practice PerfectMail™ will contact the client for permission to perform such actions.

25 Glossary

AfriNIC
AfriNIC is the Regional Internet Registry (RIR) for Africa.

APNIC
APNIC is the Regional Internet Registry (RIR) for the Asia/Pacific region.

ARIN
American Registry for Internet Numbers. The Regional Internet Registry (RIR) providing services for Canada, many Caribbean and North Atlantic islands, and the United States.

DNS
Domain Name System (DNS) stores and associates many types of information with domain names; most importantly, it translates domain names (computer hostnames) to IP addresses. It also lists mail exchange servers (MX) accepting e-mail for each domain.

DNSBL
DNS Black List. Any Black List that is implemented using DNS services. For example, the Spamhaus RBL list.

DROP
Don't Route Or Peer is an advisory "drop all traffic" list consisting of stolen 'zombie' netblocks and netblocks controlled entirely by professional spammers. DROP is a tiny sub-set of the SBL designed for use by firewalls and routing equipment. DROP is maintained by spamhaus.org.

FQDN
Fully Qualified Domain Name. An unambiguous domain name that absolutely specifies the machine's name within DNS. For example, mailserver.foo.com.

IMAP
Internet Message Access Protocol (RFC 1064) is an application layer Internet protocol that allows local clients to access e-mail on a remote server.

LACNIC
LACNIC is the Regional Internet Registry (RIR) for Mexico, Central and South America.

MTA
Mail Transport Agent. A term for programs that send and receive e-mail between servers using the SMTP protocol.

PBL
The Spamhaus Policy Block List (PBL) is a DNSBL database of end-user IP address ranges which should not be delivering unauthenticated SMTP email to any Internet mail server except those provided for specifically by an ISP for that customer's use. The PBL helps networks enforce their Acceptable Use Policy for dynamic and non-MTA customer IP ranges. PBL is maintained by spamhaus.org.

POP or POP3
Post Office Protocol is a protocol used by mail clients for fetching e-mail from a mail server.

Reverse DNS
A process to determine the hostname or host associated with a given IP address or host address.

RIPE
RIPE is the Regional Internet Registry (RIR) for Europe and the Middle East, including Greenland and Russia.

RIR
Regional Internet Registry. Five Regional Internet Registries exist: ARIN, RIPE, APNIC, LACNIC, AFRINIC. Each RIR provides services related to the technical coordination and management of IP address resources within its service region.

ROKSO
The Register of Known Spam Operations (ROKSO) database collates information and evidence on known professional spam operations that have been terminated by a minimum of 3 Internet Service Providers for spam offenses. ROKSO is maintained by spamhaus.org.

SBL
The Spamhaus Block List (SBL) is a real-time database of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services), maintained by the Spamhaus

Project team and supplied as a free service to help email administrators better manage incoming email streams.

Spam

E-mail that is both unsolicited by the recipient and sent in substantively identical form to many recipients. Two categories of spam exist: unsolicited bulk e-mail (UBE) messages and unsolicited commercial e-mail (UCE). UBE is bulk blasting of e-mail in contravention of anti-spam laws (e.g. CAN-SPAM Act). UBE spammers promote unethical, illegal and/or immoral activity and may also use spam to commit fraud (identity theft). UCE is e-mail used as a marketing tool. Senders must clearly identify themselves and maintain opt-out capabilities.

Spam Traps

Spam Traps are *fake e-mail addresses* that are created for the sole purpose of attracting spam. These fake e-mail addresses are published in such a way that they would only be discovered by automated e-mail address harvesters that are used by spammers. So any e-mail received by these fake e-mail addresses is treated as spam and can be used to detect the same spam when it is sent to legitimate e-mail addresses.

SPF

Sender Policy Framework is an extension to the SMTP. SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM header. This strategy helps defend against e-mail spam. SPF is defined in Experimental RFC 4408.

SMTP

Simple Mail Transfer Protocol is the de facto standard for e-mail transmissions across the Internet. Formally SMTP is defined in RFC 821 as amended by RFC 1123. The protocol used today is also known as ESMTP and defined in RFC 2821.

SSL

Secure Sockets Layer (SSL) is an encryption protocol designed to enable applications to transmit information back and forth securely. Applications that use the Secure Sockets Layer protocol inherently know how to give and receive encryption keys with other applications, as well as how to encrypt and decrypt data sent between the two.

XBL

The Spamhaus Exploits Block List (XBL) is a real-time database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, Wingate, etc), worms/viruses with built-in spam engines, and other types of trojan-horse exploits. XBL is maintained by spamhaus.org.

Warez

Is copyrighted material traded in violation of copyright law. The term generally refers to illegal releases by organized groups, as opposed to peer-to-peer file sharing between friends or large groups of people with similar interest using a Darknet.

Note:To ensure conformance and minimize ambiguity, the definitions for many Glossary items were taken from Wikipedia (www.wikipedia.org).

26 Support

If you have any issues at all, please contact our support team. You can reach us between 9:00am and 6:00pm EST, Monday to Friday. The best way to get support is to file a Support Incident on our website: http://www.perfectmail.com/support.

If you discover a PM bug, then your support incident incurrs no charge. Support incidents are intended to help customers do things more quickly and effectively or to help gather information or identify e-mail issues.

Support incidents are included in the price of the product (excluding the free version). Support packs are also available to bump this if needed. With support, if the issue is with our software or some deficiency on our part, including unclear documentation, or for customer feedback support is free. For other issues we burn or charge for a support incident.

E-mail Addresses:
Sales: sales@perfectmail.com
Support: support@perfectmail.com

Phone Numbers:
Office: +1 905 451 9488
Toll Free: +1 888 451 3131
Facsimile: +1 905 451 7823

Mailing Address:
PerfectMail™
15 Claypine Trail
Brampton, Ontario
Canada L6V 3L8

Web Site:
http://www.perfectmail.com